# An island at risk: Britain's undersea infrastructure and the threat beneath

*By Marcus Coetzee, April 2026.*

Winston Churchill famously said that, "The only thing that ever really frightened me during the war was the U-boat peril." He realised how vulnerable Britain's supply chains were to underwater attacks, much the same as they are today.

The United Kingdom is heavily reliant on a multitude of undersea gas pipelines, fibre-optic cables and power lines. This infrastructure is vulnerable to landslides on the ocean floor, accidental damage from fishing trawlers and ships dragging anchors, and deliberate sabotage.

Antagonistic countries or factions can sabotage these cables and pipelines, causing massive damage to the UK's economy and services. These events would have significant negative downstream effects on the wellbeing of people and communities, creating shocks such as the Great Recession or the COVID pandemic, depending on the extent of the damage.

National infrastructure is not impervious; it can degrade, collapse or be sabotaged with critical consequences, as anyone who has lived in a developing country for any extended period will tell you. It must also be protected, or it will disappear.

This undersea vulnerability has been on my mind ever since I read about explosions in the Nordstream gas pipelines during the early stages of the invasion of Ukraine. Subsequent events like Chinese ships dragging anchors and damaging fibre-optic cables, and Russian spy ships surveying UK cables and pipelines, confirmed this risk.

My recent essays on the UK's energy policies and government income further highlighted these vulnerabilities and the negative consequences should they be exploited.

This new essay builds upon the theme of the vulnerability of the UK's infrastructure. It describes the UK's reliance on its undersea cables and pipelines and how antagonistic countries can damage them. I also discuss how the UK government might mitigate this risk.

## 1. Islands provide unique opportunities and vulnerabilities

It has taken me a while to make sense of the strategic merits and risks of large islands after living on the large African continent for most of my life.

Islands provided a military advantage in ancient times. Ships were not as robust and reliable, and sea voyagers were fraught with dangers. It took considerable time and effort to ready a fleet to invade the country. The weather had to be perfect, or the ships might sink; the fleet might even get lost. The English Channel, Atlantic Ocean and North Sea act as a very wide moat around a castle.

Being on an island also helped defend against the attacks of the Spanish Armada (1588), Napoleon (1803-1805) and the Nazis (1940). These attacks could be anticipated because of their industrial scale and obvious preparations. This was different from the Vikings, who used to establish bases in Britain and nearby islands, and then launch localised invasions along the coast and up large rivers.

I loved playing Age of Empires 1 and 2 when I was younger, and preferred to choose a seafaring nation with a large island base for these reasons. It was much easier to defend than the other options, but I had to rapidly build up a fleet of ships and place defensive towers along the coastline.

Being on an island encourages a nation to develop seafaring capability. Ships are needed to explore, fish, trade, defend and conquer. Britain's navy was especially renowned from the mid-19th century through to the end of World War I, when it downsized due to austerity measures and naval treaties that limited ship numbers.

But living on an island also creates vulnerabilities, most notably with supply chains and the need to bring in raw materials and goods from elsewhere. During World War II, the German U-boats (i.e. submarines) effectively isolated Britain, sinking thousands of supply ships from North America and elsewhere, hence Churchill's earlier quote about the U-boat peril. Over 2,200 Allied merchant ships were sunk by German submarines during the prolonged Battle of the Atlantic (1939-1945).

The National Security Strategy (2025) acknowledges the need for the UK to protect its territory: "An island nation needs to be able to control its borders and maritime environment. Security at home requires monitoring and managing who and what enters our waters and airspace….Our territorial security therefore begins at sea – from our ability to stop criminal gangs and deter hostile states to the import of food and energy supplies."

While times and technologies have changed, the risk to the UK's supply chains remains present. Except that rather than U-boats, the threat is more likely to be dragging anchors and swarms of underwater drones.

## 2. The UK has a mass of undersea infrastructure

There are many more undersea fibre-optic cables, gas pipelines and electricity cables than I had anticipated when I started researching this essay, which substantiated my sense of their vulnerability.

**There are approximately 62 fibre-optic undersea cables for data and telecoms** travelling to North America, Europe and the Pacific, with several reaching Africa and Asia. More than 95% of the UK's internet traffic travels through these cables, with the remaining coming from satellite. I'm very aware of how these cables can break and stop working. South Africa, where I lived before moving to the UK, was connected to Europe by several cables, such as the 14,500km cable that links South Africa to Europe and serves many African countries.

There were significant breaks due to underwater landslides, ships dragging anchors and fishing trawlers. These led to internet and telecommunications problems that took months

to fix and caused massive, frustrating delays as digital traffic was rerouted, often via Asia. I would often see Léon Thévenin, a cable repair ship, being docked at Cape Town harbour when we went for coffee at the waterfront, getting some respite and resupplying, between doing up to 10 repairs per year.

**There are also six main undersea gas pipelines:** three from Norway, one from Belgium, one from the Netherlands, and one from Britain to Ireland. More than three-quarters of the UK's piped gas imports come through these pipelines.

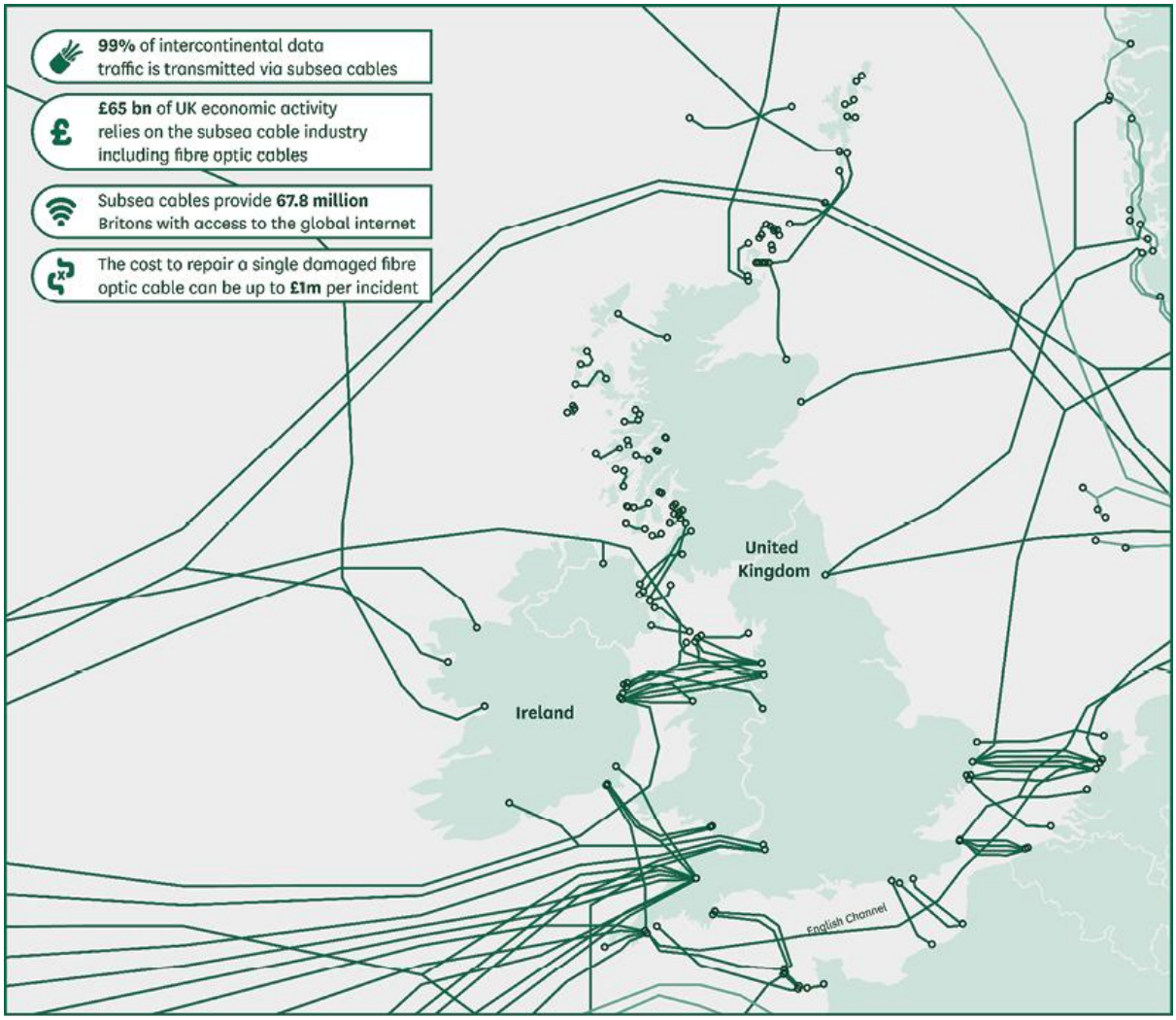
**There are 10 main undersea electricity cables, including the ones under construction.** These connect Britain with France, Belgium, Denmark, the Netherlands, Norway, Northern Ireland and the Republic of Ireland. These have a combined capacity of over 10GW, which is roughly equivalent to the UK's entire current nuclear infrastructure.

The above-mentioned undersea cables and pipes are buried approximately 1-3 yards below the seabed in shallow waters, where anchors and fishing activity may damage them. In much deeper waters, such as one mile under the sea, these cables simply lie exposed on the ocean floor since it is impractical and too expensive to bury them.

One of my friends is a geologist who specialises in surveying the ocean floors for companies that lay undersea cables and pipelines. She spends significant time on specialised survey ships and examines photos and scans of the sea floor, and rock samples. I've been impressed by how accurately she said the seafloor is mapped along critical pathways. She's even told me stories about re-routing undersea infrastructure around shipwrecks, crashed aircraft and unexploded ordnance.

These undersea cables and pipelines connect to a smaller number of terminals (nodes or landing points) on Britain's mainland. For example, the Bacton Terminal in Norfolk channels one-third of the UK's natural gas. While it is more efficient to run, and potentially easier to protect a smaller number of locations, it also increases the overall risk if a node is damaged.

The map below, taken from the 2025 JCNSS report on subsea cables, illustrates just how concentrated this infrastructure is, especially around Southwest England and the English Channel. The same report estimates that £65 billion of UK economic activity relies on the subsea cable industry alone.




*Source: JCNSS, Subsea telecommunications cables: resilience and crisis preparedness, 2025.*

## 3. The ability to destroy undersea cables, pipelines and tunnels is well-established

Most modern militaries with strong navies have the means to survey and destroy undersea cables and pipelines. It is fair to assume that potential enemies of the UK have prepared and roleplayed such scenarios, and evidence that these plans exist. They are simply kept on standby and updated periodically, or as needed. This is what I would do for all the critical infrastructure of my potential antagonists if I were in charge of the military. Hence, it is fair to assume that military leaders are ahead of me in their thinking.

It is also clear that the UK government is acutely aware of this risk, based on the 2025 briefing to the Joint Committee on the National Security Strategy.

Here are some examples of undersea events that directly impacted the UK to demonstrate the severity of this problem:

- In 2012, a fibre optic cable connecting the North West Highlands, Skye and the Western Isles was damaged, which impacted phone lines, internet and cash machines, including 999 calls.
- In October 2022, cables connecting Shetland with the Faroe Islands and then with the Scottish mainland were cut in quick succession, leaving the islands' 22,000 residents without internet or phone connectivity. A Russian scientific research vessel, the Boris Petrov, was tracked in the vicinity at the time. This happened just weeks after the Nord Stream pipeline was destroyed.
- In July 2025, a cable between Orkney and the Scottish mainland was damaged, presumably by a fishing trawler, taking down internet, telephones and even the Balfour Hospital switchboard.
- Near miss: In January 2025, the Royal Navy monitored the Russian spy ship Yantar, which spent several days positioned directly above transatlantic cables off the Cornish coast. Yantar is equipped with cable-cutting tools and its own submersible, and this was the second time in three months it had entered British waters.
- In September 2025, the UK and several other countries experienced significant disruptions to online services after multiple cables were cut in the Red Sea, affecting Microsoft Azure, among others. The damage was attributed to either accidental damage or Houthi activity. I vividly remember the frustrations this caused.
- Most recently, in April 2026, Defence Secretary John Healey revealed that the Royal Navy had spent over a month monitoring three Russian submarines in the North Atlantic. One was a nuclear-powered attack submarine, used as a decoy, while the other two were specialist deep-sea submarines from GUGI, Russia's Main Directorate for Deep Sea Research, specifically designed to survey underwater infrastructure in peacetime and sabotage it in conflict. Reading about this finally pushed me to write this essay.

The vulnerability of undersea cables and pipelines is also demonstrated in recent examples from elsewhere, starting with the Nord Stream sabotage:

- In September 2022, several months into the Ukraine war, the two Nord Stream gas pipelines from Russia to Germany were blown up in the Baltic Sea. The evidence now points strongly toward Ukraine. This event vividly reminded me of the vulnerability of undersea pipelines.
- In October 2023, a gas pipeline and data cable between Finland and Estonia were damaged by a Chinese cargo ship, the Newnew Polar Bear, which dragged its anchor across the seabed for over 100 miles. The ship was later found at a Russian port with a missing anchor, and anchor paint matching the cable was found on the vessel. It was subsequently spotted sailing alongside Norwegian gas pipelines.
- In November 2024, an internet cable between Lithuania and Sweden was cut, and then, within 24 hours, another cable between Finland and Germany was cut in the same area. A Chinese cargo ship was tracked by satellite and shown to have dragged its anchor, also for over 100 miles across both cable routes.
- In December 2024, a power cable between Finland and Estonia was cut on Christmas Day, along with four telecommunications cables simultaneously. A Russian shadow

fleet tanker was seized by Finnish authorities after a lost anchor was recovered and matched to the vessel.
- In December 2025, Finland seized another vessel travelling from Russia to Israel after it was caught dragging its anchor over an undersea telecoms cable between Finland and Estonia.

There is too much coincidence for all this to be accidental, but legal processes require a level of intent to be proven, something which is difficult to do in these international courts. This makes it notoriously difficult to attribute blame to another country or faction. But what is very clear is that most of this damage was caused by ships “accidentally” dragging anchors rather than the targeted explosions at the Nord Stream pipelines.

## 4. Drone warfare versus underwater infrastructure

The war in Ukraine has demonstrated the power of airborne drones carrying explosives and guided by humans. The volume and nature of drone warfare is beyond what most people imagine. Ukraine produced over four million drones in 2025 and intends to produce over seven million drones in 2026. And since early 2025, both Ukraine and Russia have been experimenting with AI-controlled drones.

Counter-drone technologies have also evolved. Electronic warfare involving interfering with radio signals to drones has evolved, as have physical tools like anti-drone nets and missiles. The success of electronic warfare in defending against drones is one of the reasons for drones using fibre optic cables of between 10 and 30 miles long to reach their targets. (Fibre-optic cables enable constant communication between the controller and drone, whereas radio signals can be disrupted.) Over 35 million miles of fibre optic cables were ordered and consumed by Ukraine in 2025 alone.

Ukraine has also started using undersea drones. In December 2025, an undersea drone called the Sub Sea Baby struck a Russian submarine in the port of Novorossiysk. It is a submersible variant of the surface Sea Baby drone, which has a range of over 900 miles. The range of the undersea version has not been publicly disclosed. This means that someone standing on a beach in Europe could possibly attack Britain’s Eastern Coast and bypass most harbour security. It could equally attack wind farms like the massive one being developed at Berwick Bank on the East Coast of Scotland. Ukraine’s use of an undersea drone is the precedent most relevant to this essay since it demonstrates their potential and targeted destructive power.

AI-controlled drone swarms have also evolved considerably, which is even more impressive and terrifying. For example, in 2026, China put on an airshow of over 22,500 drones that created synchronised aerial patterns in colour. Now imagine if they were all equipped with explosives, safeguards were removed from the AI, and they had protections against electronic warfare. I’ve read enough military SciFi books in my life, one of my favourite genres, to know how this can evolve and change the rules of engagement.

Drone warfare in the Russia-Ukraine conflict has focused on airborne attacks on military units and bases, and key infrastructure. Drones have sought to terrorise populations and generate fear. What we haven't yet seen on a mass scale is drone warfare moving under the sea. This is partially because these battle fronts are primarily land-based. In contrast, when two powers engage in conflict across the sea, then water-borne and sub-sea drone tactics will rapidly develop.

It is reasonable to assume that attacks aiming to undermine the UK would evolve to make extensive use of underwater drones, as it's an island that relies on undersea pipes and cables for gas, electricity and telecommunications. While ships dragging anchors have so far proven simple and effective, it is not something that can be done at scale. Ships can be tracked, blocked and boarded, especially if hostilities break out. This is why I believe that underwater sabotage and counter-drone warfare will emerge out of this. I understand that there are additional limitations (and opportunities) compared with airborne attacks. Churchill's concern remains equally valid for underwater drones.

## 5. Economic consequences would be severe, if not terrifying

Island nations like the UK rely heavily on trade to get the raw materials and finished products that their economy and populace need. These tend to arrive by ship, hence an opponent like Nazi Germany in World War 2 would try to prevent these supplies from arriving, thereby strangling the economy and undermining the wellbeing of the population.

While this is not the focus of this essay, the same principle applies to sabotaging undersea cables and pipelines - it would constrain internet and telecommunications with parties in other countries, and undermine access to cloud-based apps, databases and other services. Ever since my brief foray into the field of cybersecurity, I'm much more mindful of the fragility of digital systems and the need for multiple layers of defence. Even the app that I use to get into my gym may not work because its underlying database is hosted on a foreign server. A damaged gas pipeline or terminal would reduce gas supplies significantly. Remember that gas is used to power the turbines needed to generate electricity, and it is also used to operate machinery in factories, warm our homes and buildings, and cook food.

Significant damage to the UK's undersea gas pipelines, power lines and fibre-optic cables would have a catastrophic impact on the economy and on a multitude of other everyday services. But as far as I can tell from my research, there is no single comprehensive published assessment on what the coordinated damage to the UK's undersea infrastructure would cost, and what its impact would be, so I've selected three examples to help illustrate my point:

First, the National Risk Register 2025 addresses risks to national infrastructure resilience, including the potential disruption of undersea fibre optic cables, particularly the transatlantic ones, through accidents and deliberate sabotage. It recognises the downstream impact on communications networks, financial services, supply chain management and payment systems. However, the register treats this within a broader framework of infrastructure

vulnerability rather than as a standalone risk. This understates the specific and concentrated threat to the full set of undersea cables and pipelines.

Second, the Joint Committee on the National Security Strategy (JCNSS) 2025 report to the House of Lords and the House of Commons intentionally omits sensitive findings since the authors didn't want potential enemies to get hold of this intel. The report did, however, highlight that sabotaging multiple cables simultaneously could take down the internet and large parts of the retail and travel sectors within minutes, and that the financial services sector represented the greatest concern.

Lord Hutton, the former defence secretary for a Labour government, said, as quoted in National Security News, that "Undersea cables are now the most important part of our national infrastructure. Without them, we'd be propelled back almost into the dark ages"... "The fundamentals of national life today would be at risk - how our health service operates, how our banking system operates.

Third, the financial sector relies heavily on subsea cables, and London is one of the world's most important financial hubs. The JCNSS inquiry cited estimates that around $1.5 trillion (approximately 23% of global cross-border financial flows) is transmitted daily via data networks that rely on subsea fibre-optic cables. London is a major global financial centre and plays a significant role in this international transaction flow. Speed is everything in the financial sector, especially when trading financial instruments. Extended periods of latency, or disruptions lasting hours, can cost billions of pounds in lost opportunities.

The risks I've highlighted so far in this essay are so potentially catastrophic that the British parliament is not fully aware of them, lest the information gets leaked and potential enemies refine their strategies.

## 6. Protecting against attacks and sabotage

The big question is how the UK government would protect this underwater infrastructure and mitigate any significant or large-scale sabotage. I have always believed in the value of upstream and system-level solutions to downstream and component problems, and that is where the government must focus.

**Monitoring and defence**

The National Security Strategy (2025) states that, "The Royal Navy will take a leading and coordinating role in securing undersea infrastructure and maritime traffic carrying the information, energy and goods upon which we depend."

To provide the Royal Navy with the intel it needs, there must be intensive and widespread monitoring of these undersea pipelines, powerlines and fibre-optic cables. This will reveal when risks are present. We cannot assume that no one will ever take hostile action against them. It is unwise for leaders to assume this infrastructure will be safe because it's under the water. Monitoring should involve a mix of passive approaches (e.g. sensors, satellites, radar) and active methods (e.g. drone, submarine and ship patrols). There are currently sensor systems capable of identifying disruptions to cables within a 1m distance and then

potentially cross-referencing this with satellite information - this is a component of the NATO HEIST programme, which also explores re-routing traffic through satellites in emergencies.

The Royal Navy needs to build the capacity to monitor and defend its widely dispersed undersea network, bearing in mind that it would be too expensive to build and operate the number of large ships required. The navy has one Multi-Role Ocean Surveillance Ship, the RFA Proteus, which entered service in 2023, and is specifically designed to research and protect important undersea infrastructure. Another one is being planned for the early 2030s. From what I've read, Russia has several ships with submersibles capable of researching and attacking undersea infrastructure through methods such as placing limpet mines on pipes and cables.

My instinct is that this battlefront will become drone-focused, as I hinted at earlier in this essay. Fortunately, this seems to be what the Navy has been investing in, though perhaps not at the scale I hope for. The UK government's Atlantic Bastion programme aims to connect the surveillance of ships, submarines, aircraft and unmanned vessels into a digital spider's web that can detect potential undersea threats. The government is also developing the SG-1 Fathom, an autonomous underwater glider that is virtually undetectable by passive sonar and capable of remaining submerged for up to 90 days. Potential enemies of the UK are likely to be investing in similar infrastructure of their own, starting an underwater arms race. But there are simple solutions that mustn't be overlooked amidst these expensive programmes. To monitor and respond to threats across this distributed network of tens of thousands of miles of pipes, cables and powerlines, a larger fleet of smaller warships would also be required, each equipped for electronic warfare and carrying underwater drones to deploy.

**Repair and redundancy**

Since cables will be damaged in any conflict, the UK government must invest in the capacity to rapidly repair underwater cables and pipelines. Unfortunately, the government owns no cable repair ships whatsoever. This is perhaps the starkest single fact in the whole vulnerability picture. Although repair ships are on standby, all are commercially owned; it would take them up to 24 hours to leave port, and as long as 10 days to reach and repair cables in the Channel or Irish Sea, and up to a month in the Atlantic. The UK government should certainly develop its own repair ship, as parliament recommended, and then pay to reserve the capacity of a private service, much like the United States government has done with SubCom, the US cable repair company.

To build redundancy into the system, it is counter-intuitively necessary to have more cables, pipelines and powerlines than is normally needed. These would need to connect to the UK mainland on different nodes. While this is not economically optimal, it would create surplus capacity should something be damaged, and the additional nodes would spread the risk. All the eggs would not be in one basket, and there would be spare eggs in case some break.

**Energy and resilience**

To prevent any lasting damage caused by disrupted gas pipelines and other supplies, the UK needs to develop more self-sufficient energy infrastructure with less reliance on oil, gas and electricity imports. The need for this has become clearer as recent conflicts have demonstrated how quickly energy supplies and prices can be disrupted. My essay on the UK's energy policies recommends a foundation of nuclear power combined with renewable energy sources. I also recommend that the government directly invest in this infrastructure as opposed to simply granting licences and trying its best to tax multinational companies.

Finally, there is value in developing the means to localise financial and internet infrastructure in an emergency, or to switch across to other modes like Starlink satellites. Finland, Sweden, Norway, Denmark and Estonia have begun rolling out offline card payment systems as a backup if internet connections fail. These encrypt financial transactions on payment devices, which then synchronise with the financial network once they are back online. The UK has focused rather on protecting its financial infrastructure and resorting to cash transactions in emergencies.

# 7. Conclusion

My biggest takeaway from this essay is that the UK is very reliant on undersea gas pipelines, power and fibre optic cables. While the risks are minimal during peacetime, some of the UK's potential enemies have developed the knowledge and tools to sabotage this undersea infrastructure en masse. It is reasonable to assume they have prepared for this scenario and are ready to trigger it should it ever be required.

Because the consequences of such sabotage would be so catastrophic, and potentially take years to fix, negatively impacting the economy and the services we consume, it is worthwhile giving this risk the full attention it deserves. As with most upstream or system-level risks, they seem distant and far into the future. This makes it much more difficult for leaders and policymakers to generate the level of urgency required, and to allocate the budgets when there are so many urgent competing priorities and visible downstream problems shouting for attention.

My hope in writing this essay is to gain a clear understanding of this problem and the types of solutions that a government might use to mitigate the risks. Having lived in Africa for most of my life, I'm acutely aware of how national infrastructure can break down and what happens when this occurs, and then how long it takes to fix things again.

Churchill would likely have seen this threat emerging; it would be on his mind and possibly give him sleepless nights. This island nation that marshalled the courage and resources to fend off the U-boats will need to give equivalent seriousness to the risks posed by the emerging battlefront of undersea warfare.