



Europe's Real Front Line Is Out at Sea

Sean Tan



RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Europe's Real Front Line Is Out at Sea

By Sean Tan

SYNOPSIS

In Europe, debates on security continue to be dominated by questions of rearmament. However, rearmament without maritime infrastructure resilience exposes Europe to Russia's subtle weapons.

COMMENTARY

As [concerns](#) about the United States' reliability as a security partner continue to mount, it is known that European nations are urging the modernisation of their armed forces and expansion of national defence industries for greater self-reliance. At the centre of this political debate lie [aircraft](#), [tanks](#), and [artillery](#), underpinned by [ambitious pledges](#) of new spending.

Here, policymakers across the continent have reached for an obvious security lever – military rearmament. Besides a direct and pragmatic response to the growing possibility of kinetic conflict, the above policy appears logical as a political expedient. National defence strategies that emphasise military ordnance are likely to garner multipartisan support, due to the popular perception that such hardware provides a tangible deterrent against aggressors, besides being a useful tool for projecting power. However, Europe's adversaries are probing it in domains less visible than the traditional battlefield.

Maritime Infrastructure as Strategic Terrain

Offshore energy infrastructure is one such domain of strategic competition. Such infrastructure (e.g., [wind farms](#) and even [solar panels](#)) currently anchors several European states' transitions to renewable energy. However, similar to [undersea communications cables](#), many offshore energy projects are [privately owned](#) and [lightly monitored](#), and therefore vulnerable to interference.

In 2023, observations of Russian naval vessels monitoring offshore wind farms and undersea cable routes in the North Atlantic highlighted the disruptive potential of coercion in the maritime domain. Investigations revealed that the above infrastructure had been systematically mapped by Russian “[fishing vessels](#)” equipped with hidden military communications and surveillance equipment. This suggested preparatory work for potential sabotage, where the Russians can disrupt energy connectivity during a crisis to amplify uncertainty and political pressure.

Breach of a Norwegian Dam: Further Opening the Floodgates

More recently, the [cyberattack](#) on a Norwegian hydropower dam in April 2025 demonstrated how adversaries exploit the above domains, which Europe has been slow to secure. Norwegian intelligence revealed in August that Russian hackers had penetrated the dam’s control systems and opened its floodgates, releasing thousands of litres of water per second for several hours.

While the incident caused limited physical damage, its strategic significance is profound. Firstly, it underscores that critical energy infrastructure is susceptible to digital intrusion. Secondly, it emphasises that adversaries do not require direct kinetic force to undermine confidence in European resilience. Thirdly, it suggests that cyberattacks will increasingly target less obvious infrastructural assets, such as dams and offshore substations, rather than headline-grabbing facilities like [nuclear plants](#).

These lessons extend well beyond Europe. Across Asia, the energy transition is producing increasingly dense networks of offshore installations in both [Japanese](#) and [Taiwanese](#) waters. Maritime infrastructure resilience is hence a shared security concern for both Europe and the Asia-Pacific. In both regions, [hydropower facilities](#) and [offshore wind farms](#) increasingly rely on digital control systems. For example, Malaysia’s [Bakun dam](#) and Southern Vietnam’s [energy grids](#) are tied to centralised control systems that increase efficiency but also provide adversaries with expanded attack surfaces.

Any disruptive impact would be far-reaching, particularly as energy market shocks reverberate globally. If a comparable intrusion were to occur in the Mekong Basin or near other East Asian coastal areas, the ripple effects would be immediate and cross-border. Though still speculative, grid instability could spread through interconnected markets, undermining investor confidence and even slowing the transition to renewable energy. In densely populated coastal areas, such incidents could even blur the line between environmental disaster and strategic coercion. The Norwegian case is thus not a European anomaly, but a preview of a broader strategic challenge.

The illusion of Security Through Rearmament

In the meantime, Europe’s political reflex to growing uncertainty has been to expand military budgets. Germany’s €100 billion [Zeitenwende fund](#) and EU discussions of [continent-wide defence bonds](#) reflect this shift. However, heavy investments in

military hardware will not in themselves reduce Europe's vulnerability to energy coercion or cyber sabotage.

Crucially, Europe's ongoing rearmament drive is inextricably linked to fossil energy consumption. Heavy industries producing raw materials (e.g., steel and cement) for military machinery remain among the most carbon-intensive sectors. Moreover, fighter jets, naval vessels, and armoured vehicles are themselves overwhelmingly powered by fossil fuels, locking militaries into long-term demand for oil and gas.

Russia has a particular incentive to target Europe's renewable energy infrastructure, as these projects strike directly at Moscow's most enduring source of leverage – [fossil fuel rents](#). To Moscow, Europe's energy transition is not an innocuous climate policy, but a strategic manoeuvre. Every megawatt of wind, solar, or hydro power added to the European grid reduces its demand for oil and gas. However, as Europe's defence industries scale up, it risks prolonging its structural dependence on fossil imports just as it [seeks to escape](#) Russia's energy grip.

This contradiction is stark – efforts to deter Russia militarily are financed through industrial processes that indirectly bolster the very revenues it relies on to sustain war on European soil. From this perspective, cyberattacks on renewable projects serve a dual purpose. Operationally, they sow disruption and demonstrate the vulnerability of supposedly ["secure"](#) clean energy systems. Symbolically, they aim to instil doubt among European publics and investors about the reliability of renewables, slowing the pace of transition. In doing so, Russia seeks to prolong Europe's reliance on fossil fuels, thereby keeping open channels of influence that military rearmament alone cannot close.

Foresight Over Firepower

Moreover, US President Donald Trump's comments at the United Nations General Assembly in September further illustrate the growing distance between American exhortations and European strategic autonomy. Warning that continued European dependence on Russian oil and gas was effectively ["funding the war against themselves"](#) and suggesting secondary tariffs unless NATO states align in cutting off their energy trade with Russia, Trump's rhetoric underscored a growing American reluctance to assert leverage on behalf of Europe, particularly if Europe itself lacks the infrastructural and energy resilience to act independently.

Hence, the most effective responses do not simply lie in further militarisation, but a parallel commitment to energy resilience as a core element of security strategy. Some European leaders have since [embraced Trump's call](#) rhetorically, pointing to the EU's goal of phasing out Russian energy by 2028 and [proposals to speed up that timetable](#). Part of this would involve investments to accelerate decarbonisation and expand renewable generation, both onshore and offshore. However, other European states, notably [Hungary and Slovakia](#), have resisted on the grounds of economic and infrastructural constraints.

As such, equally critical is the protection of existing maritime infrastructure. Europe must treat offshore platforms and cables as strategic terrain, defended through

enhanced naval patrols, joint public-private monitoring mechanisms, and the development of spare routes and interconnectors. This physical security must be matched by defence-grade cybersecurity. Here, NATO and the EU can provide frameworks, but energy operators themselves must be integrated into defence planning. These operators should be held to rigorous standards of intelligence sharing and incident reporting, with regulatory regimes recognising major disruptions as national security threats.

Without a strategy to decouple rearmament from fossil fuels, Europe risks reinforcing a cycle of vulnerability. While additional tanks and fighter jets may strengthen deterrence, the illusion of security via rearmament risks obscuring structural weaknesses. Notably, Russia has consistently leveraged non-military tactics (such as cyberattacks and disinformation), as it imposes strategic costs without triggering conventional escalation. A narrow focus on rearmament risks leaving open the very avenues of pressure that Russia is most likely to exploit. Maritime infrastructure and energy resilience are therefore not just an environmental consideration, but also a decisive factor in determining whether rearmament will strengthen or weaken Europe's long-term security.

Cautionary Lessons Beyond Europe

Perhaps most notably, the vulnerabilities exposed in Europe are harbingers of risks in the Asia-Pacific, particularly as Russia [strategically redirects](#) fossil fuel exports to Asian markets. Both regions stand to gain by treating maritime infrastructure and energy resilience as a core strategic priority.

However, the threat landscapes differ in character. In Europe, risk is shaped by a clearly defined state adversary willing to employ coercion. In the Asia-Pacific, insecurity is more often characterised by ambiguity, such as piracy and/or grey-zone activities that blur the line between accident and intent. This distinction suggests that a uniform, highly militarised protection agenda would be neither practical nor desirable.

For the region's smaller states in particular, security will depend less on deterrence than on persuasion, i.e., creating conditions in which potential competitors see stability as mutually beneficial. If carefully managed, interdependence can serve as a quiet form of restraint, as incentives to disrupt critical infrastructure decrease when it is equally vital to all parties. This logic already informs some regional strategies, such as deeper energy integration between [Singapore and Malaysia](#), and even a prospective [ASEAN power grid](#). However, enmeshment carries its own risks, as Russia's swift reorientation of gas exports following European sanctions shows how easily economic ties can be repurposed for coercion.

As such, the task for Asian policymakers is to strike a balance between openness and resilience. Furthermore, while regional security debates often emphasise conventional military balance, states must not lose sight of the hybrid threats that target maritime infrastructure. Without such foresight, no amount of rearmament will shield societies from the subtler (yet equally decisive) instruments of coercion that adversaries wield.

Sean Tan is a Senior Analyst at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.

