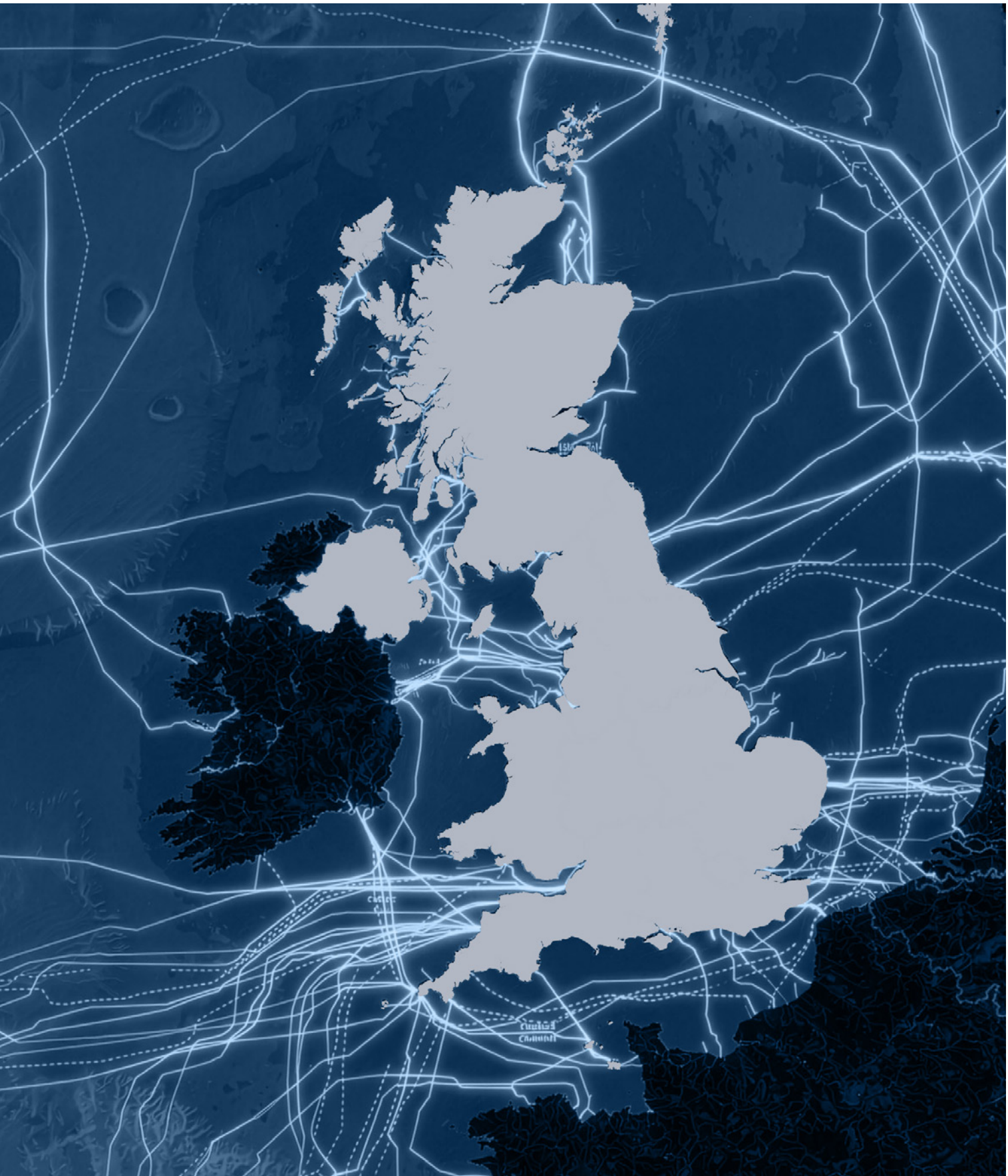
RenewableUK

New threats and new tools: reinventing energy security for an era of instability

March 2026



Authored by Daisy Powell-Chandler, Margaret Ryan.

All views expressed in this report are those of the authors, rather than of the participants and organisations consulted, and any errors are ours alone.

RenewableUK | PUBLIC FIRST | RUSI

Executive summary

Our security landscape has fundamentally shifted, and we now live in a world of geopolitical risks posed by instability from the Americas, China and the Middle East, as well as Russia. This report examines how the changing character of conflict is reshaping threats to the UK's energy system and what that implies for energy security as an element of national security.

Recent incidents, including cyberattacks, undersea cable damage and suspicious naval activity near UK seabed infrastructure, demonstrate the types of deniable, disruptive operations that can undermine energy resilience without triggering open war. The 'grey zone' nature of these attacks complicates both attribution and response. We draw on a literature review, expert interviews and a tabletop wargame run with the Royal United Services Institute to stress-test UK resilience under three plausible winter-time energy crisis scenarios.

Key findings from the report

Energy has proven to be a primary target for Russian attacks in the grey zone; vulnerabilities in our system are further amplified by severe weather, volatile global markets and unreliable international partners. While renewables have created a more distributed grid, around 30% of electricity generation still depends on gas. Because we cannot practically build redundancy for that share of supply, the UK is effectively forced to absorb gas price shocks.

The gas price shock following Russia's invasion of Ukraine required over £50bn in emergency public support to protect households and businesses. Recent tensions in and around Iran are a harsh reminder that approximately a quarter of the world's oil and gas trade relies on safe passage through the narrow Strait of Hormuz. This means that disruption far from the UK can rapidly translate into higher domestic bills as well as becoming a major political pressure point, contributing to the long term decline of energy intensive industry and eroding public confidence. As frustration grows, prolonged inaction risks undermining trust in Government, a vulnerability that adversaries can exploit without ever crossing the threshold into direct conflict.

In this report, we argue that better energy security with fewer financial risks is achievable by combining the proven strengths of the legacy system with the opportunities created by newer technologies to "reduce the leverage that enables coercion".[1] More distributed generation makes it harder for disruption to take hold, but the UK has yet to make full use of tools that can soften shocks at lower cost, such as demand flexibility and long duration storage. Rather than framing energy choices as a binary between fossil fuels and renewables, the priority should be reducing exposure to volatile global gas prices, strengthening national resilience and improving coordination and information sharing across the energy system.

Recommendations

These six recommendations for Government will help us deploy the new tools we need to meet the threats of this age:

1 Include energy, and energy spending, as part of whole of society resilience.

Just as the whole of society must be involved in national resilience, so too must the defence establishment consider energy as a core part of our society which contributes to our security. The UK should take the lead and work with NATO to develop a framework by which spending on energy system resilience can be accounted within our NATO spending targets. This is a natural extension of recent discussion at the North Sea Summit and an area in which the UK can take the initiative and work with NATO to ensure we embed security by design in our infrastructure so we can keep the system resilient and reduce costs. This would not replace core military spending, but recognise that secure power, fuel and infrastructure underpin military readiness, logistics and civil defence.

2 To maximise the strengths of both legacy and renewable energy, we should reconfigure the nation's strategic reserves for a new era by:

a. Maintaining gas storage even as our use of gas declines
b. Increasing Long Duration Energy Storage (LDES) for our electricity system to mirror our historic storage of oil and gas and ensure a diversity of LDES solutions have a clear route to market
c. Creating reserves of the physical hardware required by our energy system, in addition to existing stockpile requirements – and promoting further standardisation to improve the efficacy of this tool.

3 Integrate citizens and business into a whole of society approach to energy by encouraging participation in energy flexibility.

As renewable generation grows, our system will increasingly experience periods of abundant, low cost power. Rather than treating this variability as a problem to manage around, we should design the system to make use of it. With the right market frameworks, households and businesses can benefit directly by adopting smart technologies (such as EV charging, heat pumps, batteries and industrial processes) that automatically make use of cheaper power when it is plentiful. This in turn will create greater flexibility across the system which also improves resilience, allowing demand to shift smoothly in response to extreme events without harming consumers or the economy. Supporting electrification and access to flexibility can reduce energy bills (which remain uncomfortably high), limit the scale and cost of grid reinforcement, and strengthen overall system security — all whilst making the energy system work better for consumers and businesses.

4 Draw renewable energy into existing security channels to adapt to new threats and technologies.

The relative robustness of our decentralised renewables industry means that procedures in the event of an emergency need to evolve further. As our energy mix changes, Government should draw renewable assets more fully into security frameworks, with stronger data sharing on cyber incidents and coordinated defensive responses.

5 Re-evaluate the thresholds for strategic assets to account for new, distributed threat vectors.

As well as drawing renewables into emergency response systems, a concerted effort must be made to capture and share data from both legacy and renewables generators on the growing volume of cyberattacks that they face. This requires newer operators to step up their systems, and the Government to consider lowering the size thresholds for reporting and security measures.

6 Deepen international collaboration to protect critical undersea energy infrastructure in the North Sea.

Effective regional collaboration in the North Sea is essential for the protection of our critical undersea energy infrastructure. The recent North Sea Summit reflects the fact that that, as we are pursuing energy independence, increasing and maintaining the security of our assets in the North Sea is paramount, and it cannot be delivered without close cooperation with our regional partners. There has recently been positive progress toward this goal, but more can and must be done to combine strengths across the region.

Contents

1. What does it mean to win?

Policymakers and commentators in the energy space speak frequently about 'the trilemma' – the trade-offs between energy security, cost and sustainability. Over the past decade, as the cost of renewable energy technologies plummeted, arguments have raged over whether the tension between cost and sustainability remains. Meanwhile, energy security has largely been seen as a fixed and uncontroversial concept defined as our ability to gain enough supply to meet energy demand at all times. When we began this project, our intention was to examine the relationship between energy security and national security. The outcome has instead convinced us that there is a need for a deeper inspection of the concept of energy security, and how it needs to evolve to be better suited to the geopolitical situation in which we find ourselves and optimise the technologies now available.

The global context has become more uncertain in recent months. Trade tensions, including the use of tariffs by the United States, have raised the risk of wider economic disruption. China has shown a growing willingness to use supply chain leverage in pursuit of its strategic objectives, with implications across multiple sectors. Political and diplomatic developments elsewhere — including in the Americas and the Arctic — underline how quickly regional issues can take on broader significance.

Recent events in Iran have reinforced this picture. Around 20% of global liquefied natural gas (LNG) trade[2] and 27% of global oil shipments[3] pass through the Strait of Hormuz, highlighting how concentrated and exposed parts of the global energy system remain. Taken together, these developments serve as a reminder of how interconnected the modern world is, and how geopolitical shocks in one region can have rapid and far reaching consequences elsewhere.

Energy is often the clearest reflection of this interconnection. The UK imports around 50% of its gas.[4] Meanwhile, the list of the world's top ten exporters of natural gas[5] is dominated by players that also appear in many assessments of threats facing the UK. While Norway (not famed for its aggression towards the UK) provides a majority of our imports of gas, much of the rest is made up by LNG arriving from the US and Qatar. Russia, the second-largest global source of gas exports, is also the highest profile direct threat to the UK's national security. Russia serves as a useful illustration of the new typology of threats for which we must prepare.

Russia's 2014 annexation of Crimea began a war with Ukraine. Their full-scale invasion of Ukraine in 2022 began a complex confrontation with the West at large. The Kremlin is waging a form of hybrid warfare called *gibridnaya voyna* – rather than relying on conventional military means, this approach emphasises the use of any and all tools of state and non-state actors to undermine the West's 'military

Figure 1: Leading natural gas exporting countries in 2024, by export type (in billion cubic meters)

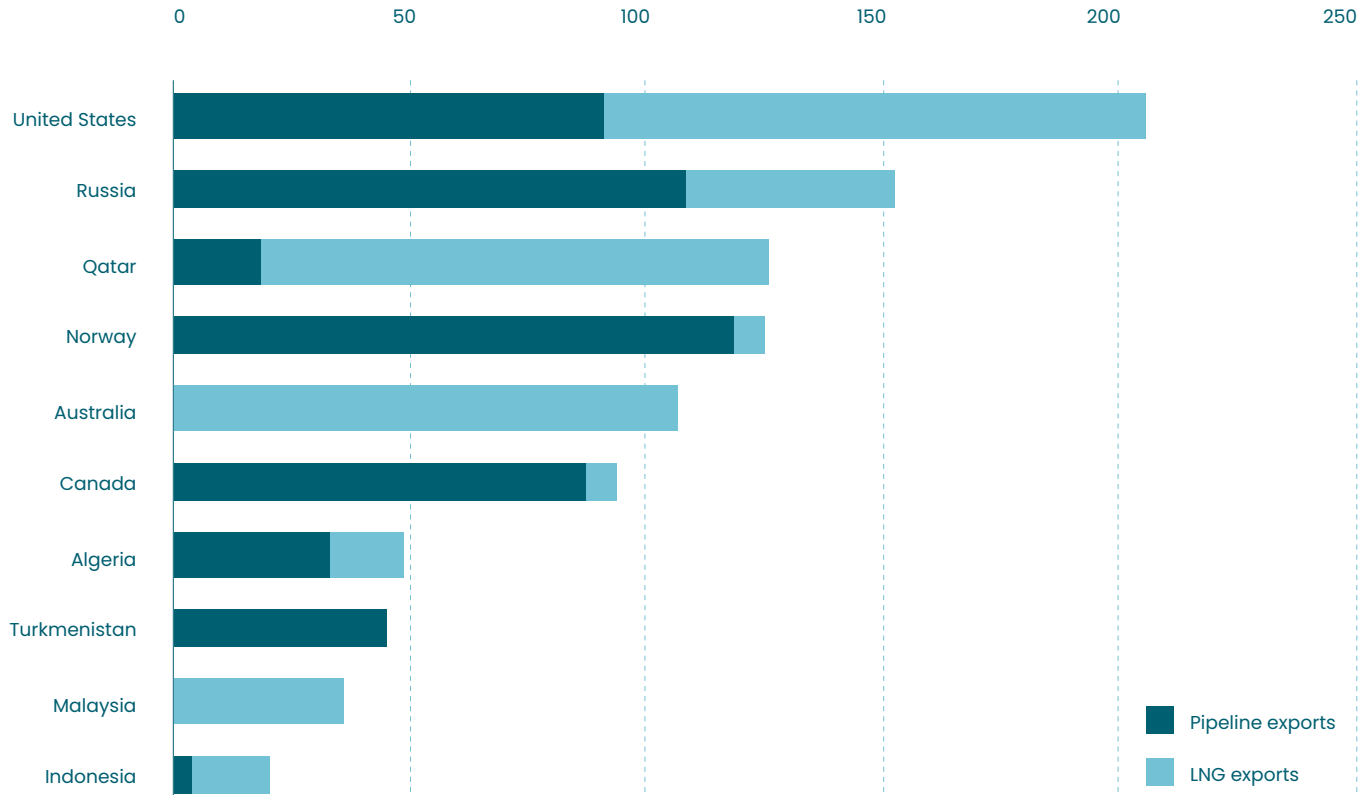
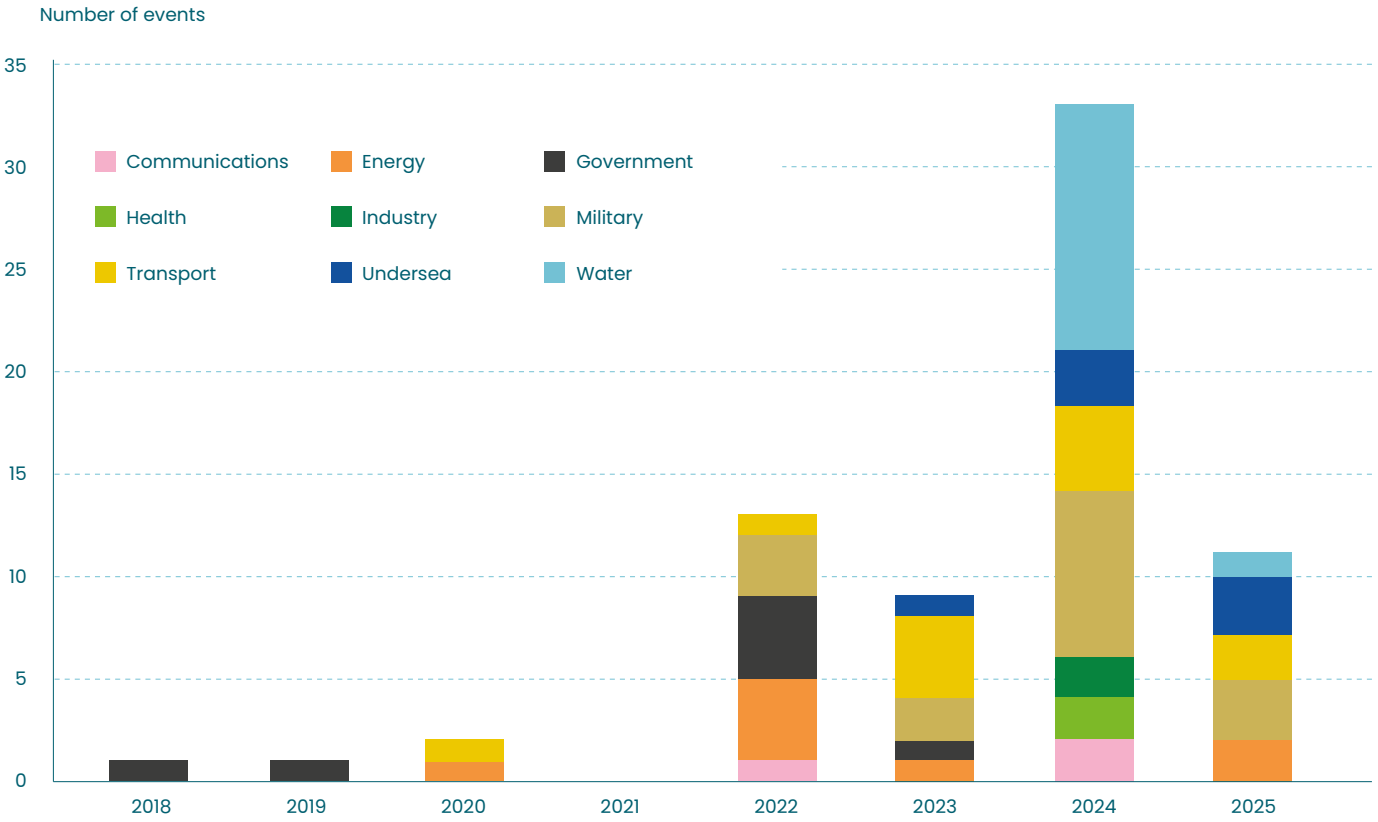


Figure 2: Frequency of Russian hybrid-warfare activity across Europe, January 2018–June 2025



and economic potential by information and psychological pressure, the active support of the internal opposition, and partisan and subversive methods.'[6] Attacks of this kind, which are disruptive but intentionally fall below the threshold of war, have come to be known as the 'grey zone' or hybrid warfare. The picture is further complicated by the involvement of non-state actors, who can pose their own threat to our security.

Russia's use of grey zone attacks is reshaping national resilience, and what it means to win. As Blaise Metreweli, the Chief of the UK's Secret Intelligence Services (MI6), said in a speech in December 2025, "We are now operating in a space between peace and war."[7] Russia is able to target nearly every sector of society – as is evident in Figure 2[8] – with little room for retaliation from the targeted state because attributing state involvement with grey zone attacks is intentionally difficult. While these attacks vary in scale, Russia has been found to be recruiting 'disposable agents' via online messaging apps such as Telegram, and paying them via cryptocurrency, to carry out many of the minor sabotage operations being discovered across Europe.[9]

An overly aggressive response to a grey zone attack runs the risk of escalation to war and provides Russia with useful information about the strengths and weaknesses of European resilience. Thus Europe, and NATO, need to adapt in order to keep pace with the changing nature of our security landscape.

Energy infrastructure has long been a primary target for aggressors, both in the grey zone and in open conflict:

- Russia has carried out regular cyberattacks on the Ukrainian energy system since the 2014 annexation of Crimea. The first major attack occurred in November 2015, in which Russian-linked groups hacked the power grid, leaving 230,000 customers without power for up to six hours.[10]
- In October 2023, the Baltic connector gas pipeline between Finland and Estonia was ruptured, in addition to two telecom cables between the two countries and Sweden. The Chinese container ship Newnew Polar Bear was quickly discovered to have been dragging its anchor for over 180km in the region, including directly over the pipeline and cables.[11] Estonia has made claims against China for compensation, but the Chinese Government maintains that a storm caused the incident.[12]
- Russian missiles and drones have taken out a significant amount of Ukraine's thermal power generation. By April 2024, 90% of DTEK's thermal capacity had been damaged or destroyed.[13]
- In December 2024, the Estlink-2 power cable connecting Finland and Estonia was ruptured, and a 100km-long drag trail was discovered to have been caused by a member of Russia's 'shadow fleet.'[14]
- The Yantar, a Russian 'oceanic research vessel', is suspected to be secretly mapping critical undersea infrastructure in the North Sea off the coast of the UK. In November 2025, it shone lasers toward the RAF pilots tracking its movements, which is both dangerous and a clear escalation from the ship's previous activity in the area.[15]

Russia is thought to be using this grey zone activity to test the most effective ways to attack the West[16]; it is therefore critical that Western energy systems are resilient enough to withstand these attacks so that we are prepared if a major escalation occurs. Russia adheres to a whole of society approach to war, so we must integrate the whole of society into our resilience.

The impacts of our lack of this resilience are already being felt; Russian tactics are taking their toll on our economy and our democracy. Our emergency support measures in response to the gas price crisis caused by Russia's invasion of Ukraine have cost the Government (and therefore taxpayers) a net total of £51.35bn.[17] This significant increase in public spending, whilst necessary, continues to impact our economy and reshape our politics.[18]

More than one form of vulnerability

The UK is particularly vulnerable to the weaponisation of energy because of our reliance on imported gas. After the discovery of gas and oil deposits in the North Sea in the 1960s, the UK Government campaigned actively to shift household heating onto gas from other vectors. The impetus for this campaign was intensified during the 1973 oil crisis, with the result that today around three quarters of British homes use gas central heating[19] – compared to 40% of homes in France.[20] But as seen in Figure 3,[21] at the start of the twenty-first century, North Sea gas and oil production fell significantly, with production down to about a third of its peak by 2022. The UK's proven gas reserves in the North Sea are now 19% of what they were in 1997 and are increasingly difficult and expensive to extract.[22,23]

Some commentators have focussed on the potential for onshore oil and gas extraction using 'fracking'. The UK's industry body for onshore oil and gas – UKOOG – estimates that if fracking is deployed then it could unlock additional gas supplies representing up to 22% of domestic gas use between 2020 and 2050.[24] However, the scale of any recoverable resource would only become clear following sustained exploration and production activity, and it remains uncertain how much gas could be extracted economically. In recent years, commercial efforts to develop fracking in the UK have largely ceased, reflecting a combination of local opposition, geological constraints, and the withdrawal of political support following seismic activity associated with operations near Blackpool. As

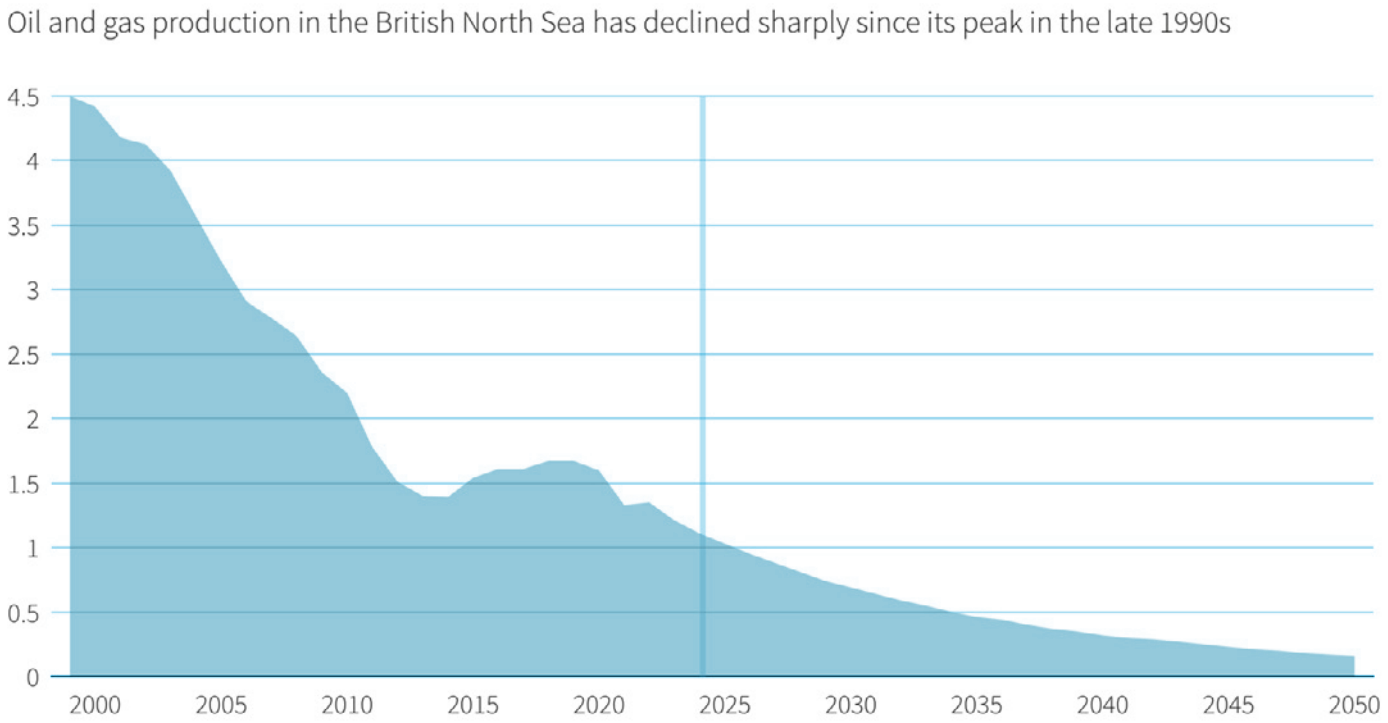


Figure 3: https://www.reuters.com/world/uk/fall-uk-north-sea-oil-rise-offshore-wind-2025-01-03/

a result, the potential contribution of fracked gas to UK energy security remains uncertain.

As a result of our increased use of gas, paired with our decreasing production of it, our imports of LNG rose rapidly after 2008 and remain high.[25]

In his 2025 Davos speech, Mark Carney, the Prime Minister of Canada and former Governor of the Bank of England, called for nations to reduce "the leverage that enables coercion".[26]We are currently moving in the opposite direction: as the North Sea basin declines, we will only become more reliant on foreign oil and gas. This will have a direct negative impact on UK energy security and leave us more vulnerable to coercion.

Greater reliance on global gas supply will lead to increased energy price volatility and make the UK less secure in a crisis – so transitioning to renewable energy is the best way to ensure continued energy security. Therefore, while there are certainly environmental motivations behind plans to decarbonise our energy system, the UK is also transitioning to renewable energy because our national security depends upon it.

When Russia invaded Ukraine, the cost of gas across the globe increased due to a mix of supply restrictions and Western sanctions. European nations adopted emergency measures within months to ensure adequate supply, minimise reliance on Russian imports, and mitigate the impact of high prices on households and businesses.

These measures included: diversifying gas supply, filling up storage, and reducing gas demand; reducing electricity demand; capping the revenue of electricity providers, and imposing windfall taxation upon fossil fuel businesses. The funds obtained from the latter two of these measures were then distributed to households and businesses grappling with high energy costs.[27]

Gas prices have now fallen substantially from their peak – though they have stabilised above their pre-crisis levels. But the UK's outsized exposure to gas price peaks, paired with the approach taken to minimise the impact of that peak on households, means that we are now saddled with an extraordinary legacy of public sector debt[28] It is not a great stretch to argue that the poor fiscal situation created by pandemic response and the gas price spike has contributed substantially to political instability in the UK in the years since, as it has constrained the ability of Government to deliver against the priorities that matter to the electorate and to ease an ongoing cost of living crisis.

This raises urgent questions about what it means to win in the context of grey zone attacks. If the UK experiences repeated gas price spikes over the next two decades, for example, would keeping the lights on, at the cost of massively increased national debt and rampant inflation really count as a win?

Global approaches to resilience

2.

Russia is carrying out a whole of society war, so the UK must ensure resilience is a whole of society endeavour. This is uncontroversial: it was a key theme in a recent speech by the Chief of the Defence Staff,[29] and features in the 2025 UK Government Resilience Action Plan,[30] Defence Industrial Strategy[31] and the Strategic Defence Review.[32] It is also reflected in the Government's 'Prepare' campaign website, which offers advice, resources and opportunities for community involvement in case of emergency.[33] Whilst it is critical that our understanding of resilience is broadening beyond defence, the role of energy underpinning that resilience is largely left out of the conversation. Meanwhile, Russia has made it clear that energy infrastructure is a key target. Resilience means much more than ensuring we have an adequate munitions stockpile in case of war. It means ensuring that all facets of British society are resilient to geopolitical and economic shocks, including but not exclusively those intentionally delivered by our adversaries. We must consider how we might mitigate against, and insulate ourselves from, the impact of ongoing grey zone attacks which impact our energy security, and therefore ultimately our national security.

Approaches to energy security elsewhere in the world

The UK's current approach to energy security was not inevitable and is not immutable. Below we have collated examples from an array of different countries and industries that demonstrate different techniques for thinking about security.

Finland: Comprehensive Security

In 1968, in response to the pervasive military and cultural threat the Soviet Union posed, Finland adopted 'Kokonaisturvallisuus' or 'Comprehensive Security' – a whole of society approach to defence in which every citizen and sector contributes to the state's national security. At the end of the Cold War, in a new era of 'peace,' some states abandoned or dialled back their total defence strategies because they no longer perceived Russia as a credible threat. Finland was an exception – the Finnish Government has never stopped considering Russia as a credible threat to Finnish national security.[34]

Finland's Security Strategy for Society is designed to ensure the defence of the seven vital functions of society:

- leadership;
- psychological resilience;
- functional capacity of the population and services;
- economy, infrastructure and security of supply and resources to maintain vital functions;
- internal security;
- defence capability,
- international and EU activities.[35]

These vital functions are considered to be the joint responsibility of the Government, businesses, civil society organisations and ordinary citizens. Since 1961, the Government has offered quarterly national-level courses for leaders outside of traditional security circles to engage with crisis scenarios and understand their roles should a crisis occur. Finland also maintains a system of civil shelters which can protect up to 4.8m people and emergency reserves of critical supplies organised by a public-private organisation the National Emergency Supplies Agency (NESA).[36] Critically, safeguarding energy supply is also clearly designated as a responsibility under the Strategy.[37]

Sweden: Rebuilding total defence

Unlike Finland, Sweden largely reduced its defence capabilities after the Cold War. In 2015, in recognition of the growing regional threat Russia posed, they began to rebuild and re-establish 'total defence': a whole of society approach which integrates the armed forces with 'civil defence'. Civil defence is a highly organised endeavour. The Swedish Civil Defence and Resilience Agency oversees 67 Government agencies which have been deemed essential to society's civil preparedness.[38] The four core objectives of their work are:

- safeguarding the most essential public services,
- contributing to the military defence's capability within the framework of NATO's collective defence and other duties,
- protecting the civilian population; and
- maintaining Sweden's will to defend itself and society's resilience to external pressure.[39]

Swedish total defence is designed to re-train the population to accept a whole of society approach to defence. Civil and military conscription have been reactivated to ensure Swedish citizens can be called up to 'do their part' in case of war, with an aim to reach 130,000 soldiers by 2035.[40] Beyond this more traditional approach to shoring up defences, the strategy also notes that 'a well-functioning energy supply is key to a society's ability to continue to function during heightened alert and ultimately war.'[41] Measures are being taken to minimise the civilian impact of potential power outages and ensure supply can be restored as quickly as possible. The Government is prioritising continued investment in fortifying infrastructure, material and personnel for quick repair, and insular supply in case of emergency. Importantly, the strategy also emphasises further training for civilians in the energy sector to respond in case of crisis.[42]

These efforts offer an important example for the UK to follow. We, like Sweden, have significantly reduced our military capacity since the end of the Cold War. While the UK has a much larger population and faces different challenges, we can learn from the lessons Sweden offers in acknowledging the criticality of a threat and mobilising the whole of society in order to address it.

Texas: ERCOT emergency alerts

The Texan energy grid, operated by the Electric Reliability Council of Texas (ERCOT), is independent from electricity grids in the rest of the United States. This allows the state to avoid federal regulations – and additional costs – for interstate energy trading, but it also means that it cannot easily rely upon outside sources of power when the grid is under strain.

ERCOT's market design makes strong use of time varying price signals. Wholesale electricity prices change through the day, reflecting supply, demand and system stress in real time. Those signals shape how different parts of the state's diversified energy system invest and operate.

As of 2025, wind and solar together supply around 36% of ERCOT's electricity, making renewables a central part of the system rather than a marginal one. Wind remains the single largest renewable source, contributing just over 20% of annual generation, while solar contributes around 14%.[43] This has helped lower average wholesale prices, while increasing the importance of flexibility as solar output falls away in the evening.

Natural gas continues to be the largest single source of power, providing roughly 40–45% of annual generation in 2025.[44] Its role has shifted over time: gas now runs fewer hours overall, but is increasingly relied on to meet peaks and to respond quickly when the system is tight. In ERCOT's market, gas is rewarded less for running continuously and more for being available and able to ramp at short notice.

Battery storage has expanded very quickly, moving from a niche technology earlier in the decade to a meaningful system resource. By late 2025, ERCOT had more than 12 GW of grid scale battery capacity online. Batteries now regularly charge during periods of low prices — often when solar output is high — and discharge into evening peaks or short lived scarcity events. While revenues have become more competitive as capacity has scaled, investment has continued, reflecting the strength of the underlying price signals.

Taken together, these dynamics have supported a more diversified system in which renewables, storage and flexible thermal generation play distinct but complementary roles. However, like any large power system, Texas is occasionally exposed to extreme weather that can place short term pressure on the grid. ERCOT manages these risks through a clear escalation process focused on maintaining overall system stability. In the first

instance, ERCOT issues voluntary conservation notices and draws on pre contracted demand response from large industrial users. Only as a last resort can it declare an Energy Emergency Alert Level 3, under which controlled, rotating outages may be used to prevent an uncontrolled system wide failure. Where this happens, it is intended to be temporary and typically lasts hours rather than days. The prolonged outages during Winter Storm Uri in 2021 are widely recognised as an exceptional case. Since then, Texas has introduced mandatory weatherisation, strengthened inspection and enforcement, and improved coordination between gas and power systems. These changes have materially reduced the risk of a repeat event, while acknowledging that no energy system can ever be completely immune to extreme conditions.

Ukraine: DTEK's swift move to decentralised energy

Despite restrictions on targeting civilian infrastructure under international law, Ukraine's formerly highly centralised energy infrastructure has been a primary target throughout the Russian invasion. DTEK, the largest private investor in Ukraine's energy sector, has been a key player in the country's efforts to recover and rebuild. Between February 2022 and April 2024, 90% of DTEK's thermal power generation, which made up a significant portion of the country's energy mix pre-invasion, was damaged or destroyed.[45] Coordinating with local defence authorities to maintain air defence against missile attacks, DTEK have been able to restore much of this capacity through a combination of rebuilt thermal plants, interconnections with Europe, and investing in renewables. Notably, in the year after the invasion occurred, Ukraine installed 19 onshore wind turbines with a capacity of 114MW. Due to tight planning restrictions, in the same year England only installed two onshore wind turbines, generating 1MW of electricity in Staffordshire.[46]

Large thermal power plants have been a primary target for Russian aggression because attacks are efficient and cost-effective for the amount of damage caused. The decentralised nature of renewables makes them a more resilient alternative. As DTEK's Chief Sustainability Officer has noted, "you would need around 40 missiles to do the equivalent amount of capacity damage at a wind farm" as you would with one missile at a thermal power plant.[47] Given the cost of a Russian missile is approximately €5 million, targeting renewables does not make sense from an economic standpoint.[48] Even if they are targeted or become collateral damage, it can take less than a week to replace a wind turbine or solar PV that has been destroyed, but it takes more than eight months to rebuild a thermal power plant.[49] Noting this resilience, DTEK has invested in diversifying Ukraine's energy mix:

- DTEK has reached a financing agreement to invest €450m to expand Tyligulska Wind Power Plant and increase capacity from 114MW to 500MW. [50]
- DTEK partnered with Octopus Energy to raise €100m to finance 100 rooftop solar and battery storage systems for Ukrainian businesses and public sector institutions.[51]
- A consortium of Ukrainian banks has agreed to invest €67m in DTEK's construction of 180MW of energy storage across the country.[52]

The Baltics: International collaboration

At the end of the Cold War, the Council of the Baltic Sea States (CBSS) was established as a foundation for cooperation in the defence and stability of the region.[53] One of their core priorities is civil security, which focuses on 'building a common societal security culture' among the Baltic States.[54]

This common culture ensures that the states have shared knowledge and are prepared to act jointly in a crisis, such as when the Estlink-2 interconnector between Finland and Estonia was cut by an anchor-dragging ship called the Eagle S. Fingrid, the cable operator, immediately reported an unplanned break in service to the Nordpool website.[55] Authorities from both countries sent vessels to investigate. Faced with bad weather, the Estonian vessel could not make it to the site, so the Finnish authorities ultimately responded to the incident. Importantly, this streamlined cooperation prevented the Eagle S from reaching Estlink-1 and causing further damage.[56]

Lessons from other sectors in the UK

National Cyber Strategy

The UK released its first National Cyber Strategy in 2016 with a focus on education, deterrence, and innovation. In order to keep up with the fast pace of technology innovation, the strategy was updated in 2022.[57] Given the ever-increasing role that technology plays in nearly everyone's daily life, the strategy was designed to build the UK into a world-leading cyber power that can take full advantage of developments in technology while still mitigating risks to security. The strategy was designed on a 'whole of society' approach to ensure that education in cyber skills is as wide-reaching as possible, as anyone using technology is at risk of a cyberattack in one way or another.

The strategy outlines a set of commitments for Government to lead by example in promoting cyber security. Since 2022, the UK has met several of these, including the establishment of a National Cyber Advisory Board as a forum for national dialogue and the establishment of the National Cyber Force, a joint defence and intelligence unit to counter cyber threats. It also sets out an expectation for accountability and proactivity from

the public sector, large businesses and organisations, Government departments, and critical national infrastructure (CNI) operators. In this, the strategy sets an example for other UK sectors by requiring whole of society participation and providing resources to make it possible.

Cyber security in the Maritime Sector

The maritime sector is one of the oldest on the planet and faces the challenge of adapting long-established systems to today's threat landscape. The sector is facing significant changes in its technology both at sea (ships, offshore structures, underwater cables) and on shore (ports). The digitisation of the sector and the convergence of information technology (IT) and operational technology (OT) present several cyber security challenges. As our energy infrastructure continues to modernise and decentralise, there is much to be learned from the maritime sector's efforts to adapt security procedures to accommodate new technologies.

Given how isolated many maritime systems have been for generations, many did not initially believe that cyber security would be a pertinent issue for the sector. This was exacerbated by the fact that a lot of the computing components were hidden or out of sight, to avoid the depredations of salt water. There was also very little clarity as to who was responsible for providing cyber security: was the manufacturer responsible for creating secure systems, the builder for choosing the most secure system, or the user for using the system in a secure manner? This uncertainty was further exacerbated by a gap between shoreside and seaside, where suppliers would maintain responsibility for the cyber security of data only up until it crossed the sea or land border, and then it was out of their remit.

The maritime sector looked to the aviation sector for existing solutions but came to the realisation that their unique security challenges require unique solutions. For example, the lifecycle of a ship is much longer than an IT server room, or an aeroplane, and maritime environments have more challenges connecting legacy systems with newer, internet-enabled systems than most other sectors. Another challenge in modernising the sector's security is establishing and acknowledging the difference between physical security and cyber security. If a system was having issues, in many instances people in the maritime sector would classify that issue as human error or mechanical error. While the impact might be similar, the risks if this was a cyber incident (malware on system or social engineering) are different, as are the ways of mitigating them. Also, the measures the sector tends to turn to for 'safety' (turn off a machine that is not working properly) can sometimes actually negatively impact the technology's cyber security.

This has been a growth area. In the last few years, standards and regulations have been changing to address the unique complexities of cyber risk in the sector. There have been more efforts to create anonymous reporting structures so that attacks and incidences can be shared across the sector for the sake of learning and improving defences internally and regionally. Technical cyber security solutions and training programmes are also increasing. This progress is still early stages as industry and Government learn what works, but the maritime sector presents an important example of an established sector making conscious efforts to move toward a more comprehensive and modern understanding of security.

Property Flood Resilience – managing disruption and minimising impacts

Security is often equated with maintaining a sense of complete control and constancy. However, security can also be found in accepting that things will go wrong and having a plan and solution prepared. The UK's approach to property flood resilience (PFR) is designed in line with the latter definition and offers lessons for the energy sector.

In 2020, the PFR Code of Practice (COP) was released by the Construction Industry Research Information Association,[58] developed in collaboration with the DEFRA PFR roundtable and several professional bodies.[59] It sets benchmarks for the construction and installation of PFR measures to improve both resistance (reducing the amount of water entering a building) and recoverability (limiting the damage if water does enter a building). This balances the sometimes-contradictory goals of getting 'back to normal' as quickly as possible with the longer-term goal of futureproofing against a repeat crisis.[60]

The energy sector can and should learn from this example. Government and industry collaborated to establish a standard for infrastructure based on the basic idea that crises are sometimes unavoidable, and preparing to minimise damage as well as prevent it strengthens overall resilience.

3. Wargaming the relationship between energy and national security

To further explore the interaction between national security and energy security, Public First organised a series of tabletop wargaming exercises. Over the course of three scenarios, we sought to understand the evolution of threats to our national security, the role that both gas and renewables play in our overall resilience, and the impact of the energy transition.

This workshop was developed in partnership with a group of relevant experts and run in collaboration with the Royal United Services Institute (RUSI). The development process unfolded as follows:

Discovery

- Conducted a literature review of credible foreign threats to UK national security which also have a demonstrable impact on our energy security.
- Carried out desk research into the most critical energy assets across the UK, complemented by interviews with expert stakeholders in energy and national security.

Refinement

- Collaborated with RUSI to select three plausible scenarios which would cause a significant crisis for the UK energy system.
- Conducted further interviews with expert stakeholders to verify the plausibility and severity of the chosen scenarios.

Wargame workshop

- Collaborated with RUSI to organise a day-long wargame workshop, hosted in their offices in Central London.
- The workshop was split into a morning session, focussed on the UK response to a physical attack on a gas pipeline in the North Sea, and an afternoon session on the UK response to cyberattacks at a gas terminal, and on one of the country's largest wind farms.

Analysis

- Conducted stakeholder interviews in order to include additional perspectives not represented on the day.
- Compiled notes from the workshop and complementary interviews to author a report detailing our findings.

The below experts were in attendance:

- **Dan Marks**, Research Fellow, Energy Security, RUSI
- **Joseph Jarnecki**, Research Fellow, Cyber and Technology, RUSI
- **Melissa Stark**, Senior Associate Fellow, Energy and Security, RUSI
- **Ian Henderson**, Sector Security, Risk and Threat Manager, NESO
- **Commander Ed Black**, Royal Navy
- **Lauren Goodwillie**, Whole Energy System Resilience Manager, National Gas
- **Roisin Cogan**, COBR Directorate, Cabinet Office
- **Emma Longhurst-Gent**, Energy Security Strategy Analyst, DESNZ
- **Paul Vinnell**, Regional Security and Crisis Manager, Equinor
- **Ben Haggerty**, Head of Whole Systems, National Grid
- **Christian Gibson**, GM UK Energy Transition, Shell
- **Christopher Dixon**, Lead Cyber Security Engineer, EDF
- **Andrew Elmes**, Head of Government Affairs, Siemens Energy

Summary of three scenarios

Context provided ahead of the scenarios:

It is the coldest January in five years, driving up energy demand across the Northern Hemisphere. To meet increased winter demand, the UK would typically lean more on LNG and gas imports to supplement domestic production. However, in response to continued Russian aggression in Ukraine, US President Trump imposes sanctions on Novatek and Gazprom. China, in the midst of delicate trade negotiations with the US, respects these sanctions.

Russia is therefore no longer exporting either LNG or pipeline gas. No longer able to meet demand via Russian pipelines, China increases imports of Qatari LNG. The EU, which still meets 14% of gas demand from Russian supply, must compete for this LNG, driving up prices to near-2022 levels.

The UK is therefore faced with a strained global market, and very high energy prices, in a period of unusually high demand. As the US's closest European ally, the country is then faced with an unattributable attack on its energy infrastructure.

Within this context, we then confronted participants with three separate scenarios. The outline of these scenarios was as follows:

Scenario one:
Physical attack on a major gas pipeline

There is a series of explosions on a transport pipeline in the vicinity of the Sleipner Riser and processing platforms. There is immediately a massive pressure drop in the system, and the UK loses 18% of its winter gas supply. It appears that explosive devices of unknown origin have targeted the undersea pipelines and infrastructure.

Scenario two:
Cyberattack on one of our largest wind farms

The wind farm control room has lost contact with all 174 of its turbines. The cause of this loss of communications is not immediately clear, but in order to protect the hardware and ensure safety while the problem is investigated, the control room shuts all turbines, dropping 1.2GW (2.5% of total demand) off the system.

It is later determined that the cause was a compromised security update rolled out by the wind farm's turbine manufacturer.

Scenario three:
Cyberattack on a major gas terminal

Malware code is found in a peripheral system of the terminal's Supervisory Control and Data Acquisition (SCADA) Master Terminal Unit (MTU). Each operator has their own decentralised SCADA system, but the MTU enables centralised oversight of the site.

The cyberattack triggers an immediate safe shutdown, and pipelines are placed in a 'no flow' state while engineers assess the likelihood that the malware has compromised safety protocols.

The terminal is one of the most critical infrastructure sites in the UK energy system. It is a gas processing and transmission hub, processing around a quarter of the UK's gas imports.

How and why we chose these scenarios

Choosing the right crisis scenarios for the workshop was an iterative process. One of the key priorities throughout the project was maintaining the integrity of the workshop by ensuring that the chosen scenarios were plausible, and relevant. We determined this plausibility by asking ourselves and expert stakeholders two key questions:

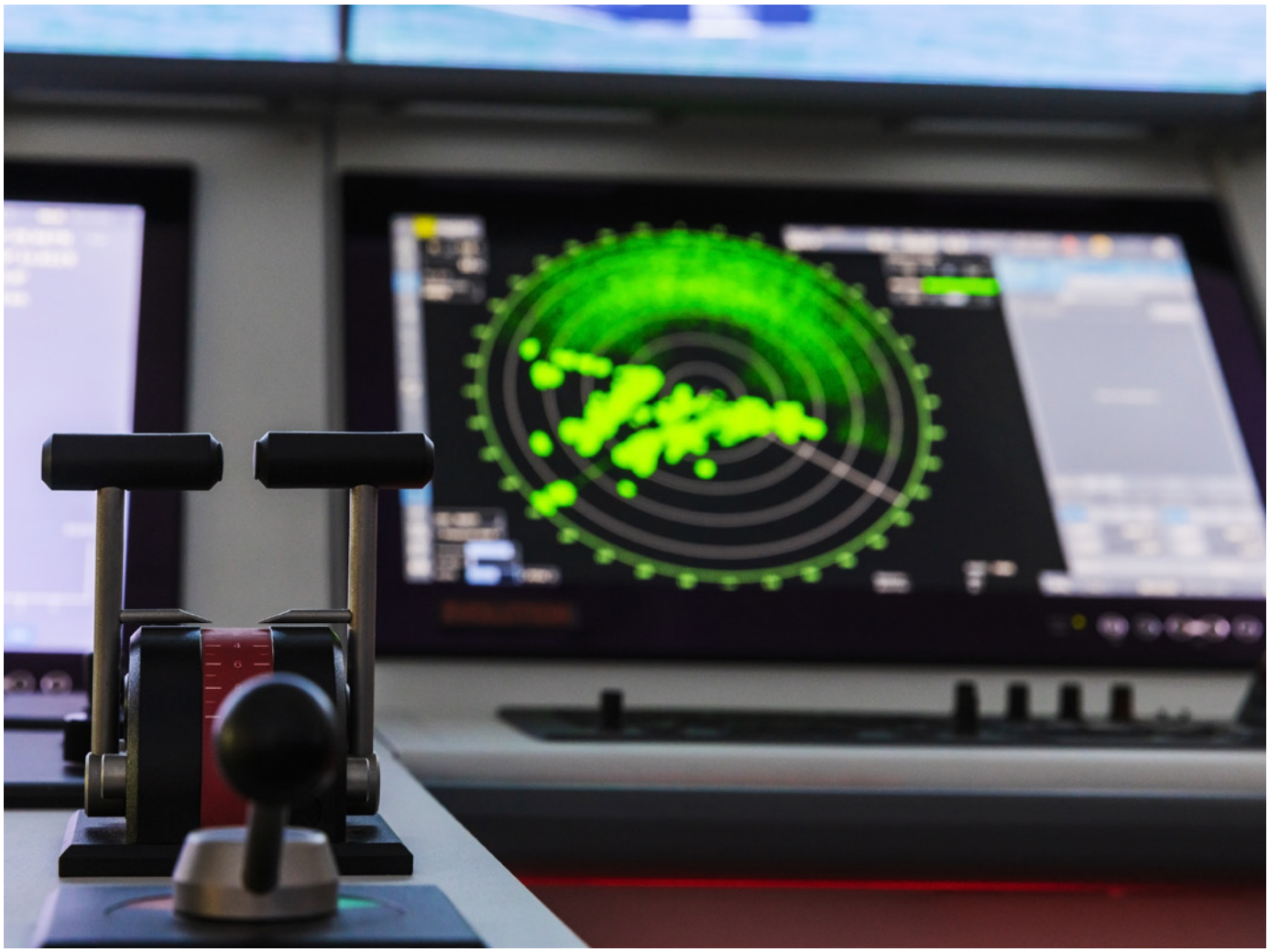
- Could this attack realistically happen, given the technological abilities and geopolitical relationships of the chosen actors?
- Is this attack, whether the method or the target, something you and/or the UK Government are concerned about?

Our stakeholder interviews provided this key insight, and we adjusted the scenarios according to their expertise. We also referred to the 2025 National Risk Register (NRR),[61] which sets out 'reasonable worst-case scenarios' for attacks on our infrastructure. This provided a guide to Government's priorities and concerns – primarily that there must be contingencies in place for both physical and cyberattacks on critical infrastructure.

We aimed to follow the NRR's example by exploring system-wide vulnerabilities and risks which impact our national security, rather than more localised risks which could be contained. This guided the infrastructure we ultimately chose to target.

Finally, we focused our attentions on scenarios in the 'grey zone' – attacks that could be carried out by an aggressor without inevitably leading to war. As we described in chapter one, this is the typical mode of attack that we are currently facing and the situation of most immediate concern to policymakers.

Amongst the scenarios that we considered but did not include in the workshop was a physical attack on a substation, which was flagged to us as worthy of exploration in the exercise. During our preparations, the National Energy System Operator (NESO) published its own review of the Heathrow substation fire, which covers that event in detail. We therefore included this report in our literature review and decided to use the time for other scenarios.



Key findings

4.

It is difficult to cause substantial damage to the UK energy system with a single attack

Our research interviews and the workshop itself revealed that it is very hard to cause substantial damage to the UK's energy system. The most difficult part of designing credible crisis scenarios for the workshop was causing plausible yet substantial damage to the system.

Early on, we were advised that in order for an attack on energy infrastructure to create a crisis for the system, we would need to layer multiple failures or aggravating factors. This is why our scenarios occur in January, when demand is particularly high. The loss of operation of any of this infrastructure in the winter would pose a significant problem, but the system could adjust. However, layered with a strained global market and subsequent high energy prices, it constitutes a crisis for the system. Stakeholders from National Gas reflected that defining a single point of failure is difficult because there is so much redundancy built into the system, both in physical and cyber infrastructure. Similarly, NESO operates the electricity system so that it can cope with the loss of the largest generating asset at any given time. It was also noted in the room that the market responds relatively quickly, dampening long-term price impact in most situations.

The weather has a substantial impact on the continuity of both legacy and renewable energy sources

Despite this broadly resilient system, we heard time and again of the importance of weather conditions. This is relatively intuitive and well-understood for renewable energy as political debate has centred on what happens to our energy security when the sun does not shine and the wind does not blow. What is less often discussed is that that our gas demand and supply are both heavily dependent on the weather. As discussed above, the UK's reliance on imported LNG has been increasing for the past two decades. LNG is brought ashore via three terminals: one at the Isle of Grain in the Medway, the other two at Milford Haven in Pembrokeshire, Wales. Cold weather increases gas demand but if that cold spell also brings rough weather in the Irish Sea, then our ability to use the Milford Haven terminals can be gravely compromised. A recently published Government consultation seeks feedback on the ways in which we could increase our capacity to import LNG[62] but these all require additional infrastructure investment and time for building work.

Gas pipelines are also liable to freeze in cold weather and disrupt supply. In 2010, Norwegian gas field Ormen Lange was shut down due to ice forming in pipelines, so the UK had to issue a gas balancing alert due to such a significant drop in supply.[63] More recently, in 2021 50% of power generation went offline in Texas after unusually cold temperatures impacted coal piles, gas wells, fossil fuel generators and wind turbines.[64] As our weather patterns become more erratic and their effects more extreme[65] and our energy mix continues to diversify, we can expect to see greater volatility of both supply and demand – and therefore greater volatility of gas prices.

Oil and gas systems are vulnerable to attack, but this has led to clearly defined emergency procedures

The centralised nature of oil and gas systems means that major infrastructure is often a single point of failure; in the right circumstances, an attack on any terminal or pipeline has the potential cause a system-wide energy crisis. In Ukraine, DTEK's thermal power plants have been a primary target for Russian aggression because it is relatively 'easy' to cut power from thousands of homes with a single missile strike on a plant. Likewise, stakeholders in our interviews and during the workshop noted that, given the significant portion of the UK's gas imports which come through a single pipeline system, one shutdown of the pipeline has the potential to cause a system-wide crisis.

UK Government and industry recognise this vulnerability, and therefore have clear emergency procedures in place for legacy oil and gas infrastructure: it is a scenario they frequently discuss and wargame. Each stakeholder knew their exact role, whom they would contact and when, and what would need to be done to get the pipeline back up and running. Gassco would call Equinor, who would call National Gas, who would call DESNZ. DESNZ would inform the Cabinet Office and work closely with other relevant departments and Number 10 to follow crisis procedures and escalation protocols. Depending on the scale of the disruption and its cascading impacts, a COBRA meeting might then be convened. In the case of the cyberattack on the gas terminal, stakeholders in the room indicated that there would be a largely similar process to communicate and resolve the issue. This preparation has made the UK energy system largely 'hard to break' and resilient against major shocks.

Renewable energy systems are decentralised, which makes them highly resilient but has resulted in lower levels of Government coordination

Renewable energy provides a core asset to our energy resilience planning because it is decentralised, and thus harder to disable. Determining a credible system-wide crisis scenario caused by an attack on renewable infrastructure was difficult. The chosen crisis – a cyberattack that leads to the shutdown of an offshore windfarm taking 1.2GW of power off the grid – should not be a system-wide emergency because the system is designed to operate efficiently even if one of our many large-scale wind power plants are not operating.

Whilst this is a positive feature of distributed energy systems such as the UK's wind and solar, it has also reduced the need for central communications structures. Responses to a cyberattack on a wind farm in the workshop focused on minimising impact on the grid: turbine shutdown can happen gradually to allow for an orderly transition to other generation sources and they could be back in operation within 'a matter of days'. These steps isolate the problem and individual operators have been working hard to improve their resilience to cyberattack. However, compared to the oil and gas scenario, because of the decentralised nature of the renewables, the response was focused on actions by the individual operator, rather than coordination across the wider energy system. In the case of a cyberattack on a wind farm, both the form of attack and the infrastructure are relatively new, and we need to ensure that the most comprehensive emergency procedures are in place to address all possible scenarios, including more robust monitoring, escalation and response procedures so that we can build industry knowledge and ensure resilience against future attacks.

The decentralisation and smaller size of renewable assets means that even when they are attacked, their disruption poses fewer threats to system stability. This has led to a regulatory structure that correctly treats renewables as a far less risky element of national infrastructure. However, in December 2025, hackers launched a large-scale cyberattack on Polish renewable infrastructure; more than 30 wind and solar farms were targeted at once in a coordinated attack.[66] They used relatively unsophisticated means, but through a combined effort were almost able to disrupt a critical mass of the country's renewable energy infrastructure. Decentralisation is a key strength of renewables, but as cyberattacks become more advanced, and our whole energy system increases its reliance on cyber infrastructure to monitor and control a complex system, there must be even clearer procedures in place to protect smaller assets from decentralised attacks and improved coordination to guard against contagion across the system.

In a known attack we have clear procedures — less so when the attacker is unclear or impact uncertain

As the nature of modern conflict changes, our emergency procedures must also change. The crisis scenarios we tested are examples of grey zone attacks – they cannot always technically be attributed, and they fall just below the threshold of being acts of war. In the case of the pipeline explosion, even if the attacker is technically unclear, the impact is certain – stakeholders in the room knew how long it would take to shut down the pipe completely, and what measures we could take to mitigate the problem.

In the cyberattack scenarios, however, there was less certainty. Cyberattacks are intentionally difficult to trace, and it is possible that malware could sit in a system for a long time before being noticed or carrying out its intended task. This results in a lack of clarity: was this an attack or a software failure? Is the perpetrator a state or non-state actor? Should we expect further attacks elsewhere in the system? With few concrete answers, the path ahead is unclear, even when the attack might ultimately be just as damaging as a physical one.

Interviews with cyber security researchers following our exercise indicated that reporting protocols within oil, gas and renewables companies require strengthening. There are pockets of good practice but often cyberattacks are repelled at working level as part of day-to-day functions and then not systematically reported upwards to executive level. This results in a lack of shared knowledge and understanding of the risks, which in turn leads to lower priority being accorded to cyber resilience at board level across the renewable and legacy energy sectors.

In this manner, the opaque and emerging nature of cyber threats results in reduced oversight by boards and Government bodies. Our assessment is that, while cyberattacks have been increasingly high profile, the lack of shared concrete examples of best practice is inhibiting senior decision-making processes and results in under-resourcing of preventative and reactive infrastructure.

The security conversation on renewables focuses on cyber security, but basic physical assets underpinning the wider electricity system also require greater consideration

When discussing the security of renewable energy, interviewees almost always mention cyber security. This emphasis is also apparent in the academic literature. The decentralisation of renewable infrastructure makes it much harder to substantially damage with a physical attack, so this is not the primary focus of security conversations. However, although it is difficult, it is not impossible to cause physical damage – particularly to subsidiary infrastructure like undersea export cables and substations. The primary cause of damage to offshore wind export cables is accidental anchor dragging from fishing ships. Because accidental anchor dragging is so commonplace, it is relatively 'easy' for malicious actors to deniably drag anchor to damage critical undersea infrastructure, as with the Estlink-2 cable in December 2024. An expert stakeholder from an offshore wind operator indicated that an attack like this was a larger concern than even a cyberattack.

Likewise, substations are a vulnerability because several wind farms, as well as gas assets, might transmit electricity via the same station, making them a critical point of failure. While a military attack on infrastructure on UK soil would of course be an act of war, infrastructure can be vulnerable to civilian sabotage. The Wagner Group has been known to recruit locally to carry out attacks in the UK. In March 2024, six men recruited by Wagner set fire to a warehouse in East London which had been storing goods to be sent to Ukraine, including Starlink satellite equipment.[67] It is clear that damage is possible to onshore infrastructure, and this needs to be part of the conversation about securing our renewables and fossil-fuelled assets.

Crisis response focuses too much on ensuring supply with too little consideration of demand or cost

In each scenario, we saw that during an energy crisis in the UK, the focus is on ensuring consistent supply – with the implicit assumption that the market must and will provide the necessary gas. Indeed, opponents of the Government's clean power agenda often contrast what they describe as the perceived reliability of gas against the variability of renewables. Recent events and this workshop reveal a more nuanced reality: that this interpretation of security means we are highly reliant on our ability to take the economic pain of significantly higher prices to maintain supply. If a crisis erupts then gas prices shoot up, and we dig deep into our pockets while trying to reduce our demand until normality returns. Following the war in Iran, we are already seeing rapid increases in gas prices and disruption to LNG production. Disruption in the Strait of Hormuz will compound the effect on the market and the cost to the economy.

This situation is no longer politically sustainable. Recent experience shows that high prices don't sufficiently or efficiently reduce demand when we are so heavily reliant on imported gas. Nor does this approach account for the long-term damage caused by periods of extremely high prices, like businesses closing, avoidable deaths and lost learning opportunities for children due to cold. Ability to pay may be the wrong mechanism for allocating scarce energy resources in these crisis situations when neither the Government nor consumers are able to bear peak gas prices.

If the UK is to reduce its reliance on expensive supply-side solutions in order to build up resilience against continuing grey zone threats, the trade-offs with cost, security, and democracy need to be made clear. As has been demonstrated, there is a direct link between maintaining gas supply and increased energy bills. We have two tools to unhook ourselves from the volatility: one is to shift our energy use further away from gas – to a substantial enough extent that gas no longer sets the price of our electricity (and is relied upon by a falling proportion of the population for heating), the second is to become more sophisticated in the way we manage demand so that when energy supplies are constrained the system has more options than simply to buy additional gas.

Of course, the Government is already set upon a strategy of reducing the use of gas in our electricity grid. Though initiated primarily for climate-related reasons, the energy security benefits of this policy are underestimated and important. In the same manner that shifting from gas to renewables insulates the UK's electricity markets from global volatility, moving from daily prices to advance

purchase contracts is also an insurance policy against price spikes. Contracts for Difference, the Government's primary vehicle for purchasing renewables capacity, also has this benefit. Both the overarching strategy and the tools by which it is being accomplished will protect energy bills from the kinds of fluctuation we have witnessed over the past decade.

The UK also has some tools to manage demand, but they are limited and rarely used. It was noted in the workshop that the Government cannot directly dictate businesses' response when the grid is strained. They are therefore limited to voluntary participation and extreme emergency measures. In 2022, NESO launched the Demand Flexibility Service (DFS), offering rewards to homes and businesses for reducing electricity use when the grid is strained during the winter period. In 2023/24, there were 2.6 million participants.[68] However, by winter 2024/25, this had dropped approximately 62% to 750,000 participants, of which a majority were households, because the incentive had dropped from £4 for every kWh saved to 60p.[69] Far more use could be made of this and similar tools. This is not a novel observation; an independent expert report on electrical standards delivered to the Government in 2020 pointed out that the deployment of flexibility technologies and systems can significantly reduce whole system costs as well as improving resilience.[70]

In a crisis, the energy system is on its own. We do not currently have a whole of society response

Psychological resilience plays a major role in whole of society approaches to resilience. The general public needs to be reasonably prepared for crisis, both mentally and in terms of resources, and needs to 'do their part' if it ever becomes necessary. Because the UK prioritises 'business as usual' for energy consumers at nearly any cost, the British public has little experience of being asked to adjust demand to accommodate a strained energy supply.

This context meant that experts in the workshop were not confident as to how the general public would react if, for example, the system could not match supply and demand and National Gas needed to issue a public appeal to turn down gas. One stakeholder argued that people's willingness to wear masks and stay home during the COVID-19 pandemic has already demonstrated that the British public will contribute to the nation's resilience when asked. However, we should be wary of comparing reactions during a sudden, national energy crisis with a global pandemic which poses a clear and immediate threat to health and safety.

In contrast, public involvement in grid management is common in the state of Texas, which has an independent grid and extreme temperatures. Texans have therefore become largely adjusted to the situation, and the state's grid operator has developed a system of alerts to communicate about reducing usage for short periods when the grid is strained. This has not harmed the Texas economy or its ability to attract energy intensive industries such as data centres. If the UK were to begin to experience similar events, Government and industry would have a responsibility to ensure the psychological resilience of the British people. This consideration for behaviour needs to be built into resilience preparations so that people are adequately equipped to respond and participate. Several stakeholders argued persuasively that, as a starting point, the Government should begin to talk more openly about the rising number of attacks that the country is facing.

The defence establishment acknowledges that a holistic defence strategy must include energy, including investment in both generation and storage, but deployment has been slow

The MoD has made slow but steady progress in integrating renewable energy onto military-owned land. In 2021, Project Prometheus was launched with the aspiration to deliver around 80 solar farms across the defence estate.[71] In 2022, Defence Equipment and Support (DE&S) identified three sites to become carbon neutral by 2025.[72] However, while they are important steps forward, these and other initiatives across the MoD have been relatively disparate.

A buildup of renewable energy on the defence estate had never been codified as a clear target for the MoD until the 2025 Strategic Defence Review (SDR) and Defence Industrial Strategy (DIS). The SDR noted that the MoD could build energy infrastructure on the Defence estate to 'reduce the department's energy bills and risk, add to National Grid resilience, and provide income streams for the Government.'[73] The DIS then proposed building energy infrastructure on the defence estate in order to meet the MoD's growing energy demands.[74] While it will take some time to see these commitments turn into delivery, we have begun to see some development take place; Great British Energy (GBE) has partnered with the MoD to roll out solar panels and micro-wind turbines to around 15 military sites across Great Britain.[75] In February 2026, DESNZ announced a £74m investment for clean energy and efficiency upgrades across 82 NHS Trusts, eight military sites and one prison. Building on its previous collaboration with Government, GBE is also investing £9m for batteries and solar panels across these sites[76]

However, given that the MoD own about 1% (342,000 hectares) of UK land holdings,[77] there is potential for much more to be done. One example could be the bringing together of NESO's Strategic Spatial Energy Plan (SSEP) and Governmental prioritisation for public land use. This would provide the direction the MoD requires to deconflict competing priorities for their own land amid wider Governmental targets such as housing and Biodiversity Net Gain (BNG).

Such energy reserves could be co-located with military facilities - or built on other resilient sites – and used to power military operations; prolong our resilience in the event of a dunkelflaute, gas shortage or price-spike at times of system stress; or to aid in black start functions. Several of our allies are already building up their strategic energy reserves across their defence estates. In the US, the Department of Energy (DOE) and Department of Defence (DOD) have established a joint programme to research and fund LDES technologies which can operate for over 10 hours at DOD facilities,[78] and an 8.5MWh battery storage system has been installed at US Army Fort Carson in Colorado.[79] In Australia, the Government has invested $13m in solar generation and battery storage at five sites across their defence estate as part of a wider energy security programme.[80]

International collaboration on North Sea security is vital but still nascent

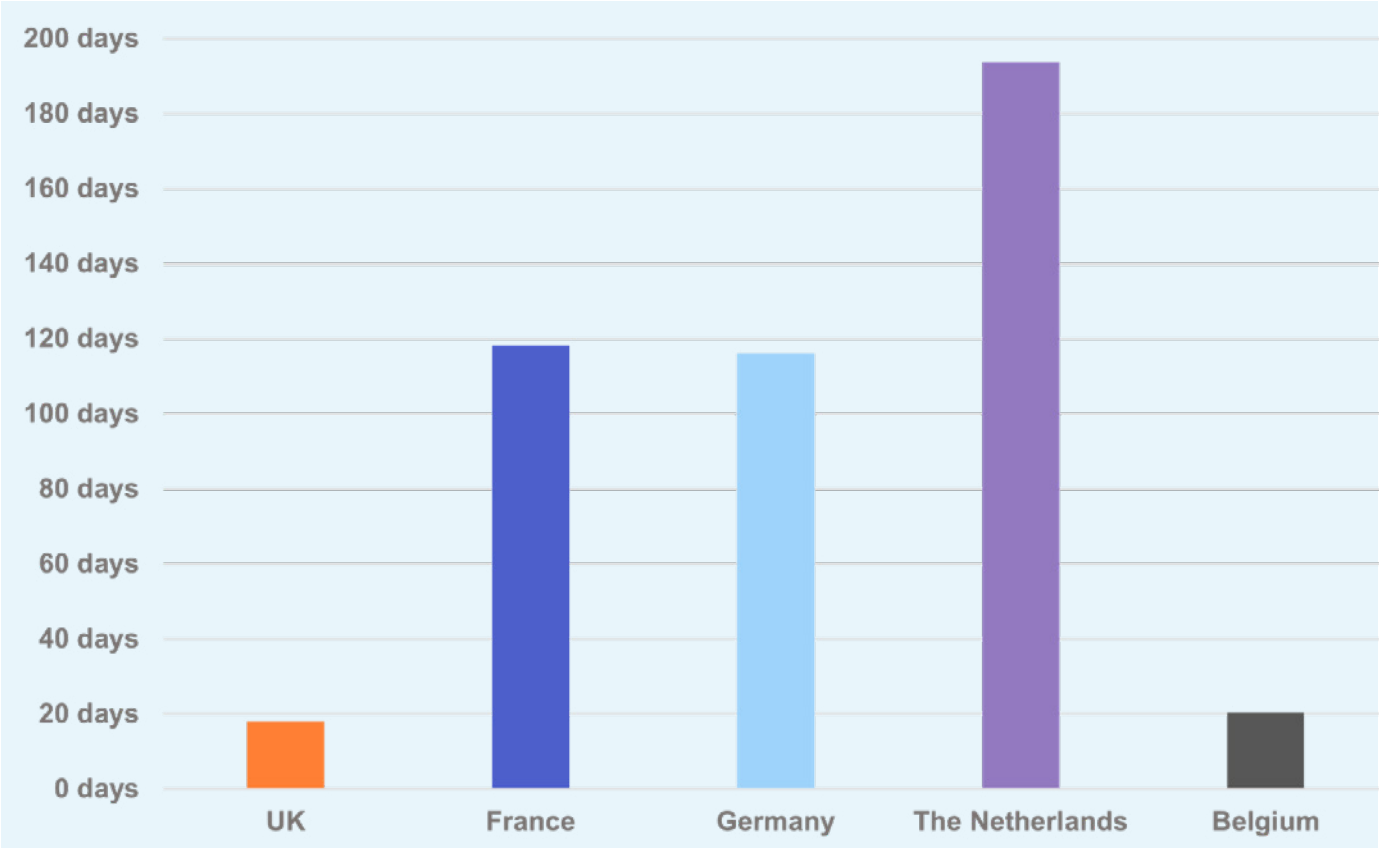
Effective regional security collaboration in the North Sea is essential for the protection of our critical undersea energy infrastructure. While there are many organisations to promote states' interests in the North Sea, these efforts need to be more integrated in order to make the region resilient against the Russian threat. The Baltic States, while they of course have a unique relationship, offer a useful example (described in chapter two) for the North Sea States (the UK, Norway, Denmark, Germany, the Netherlands, Belgium, France) around an integrated approach to defence.

There are, of course, already several collaborative measures being taken to enhance security in the region. In December 2025, the UK and Norway signed the Lunna House Agreement to combine the strengths of their navies against Russian submarines in the North Sea.[81] In a speech on 8 December 2025, First Sea Lord General Sir Gwyn Jenkins KCB OBE ADC RM introduced Atlantic Bastion, which will integrate autonomous vessels and AI into the Royal Navy to build up a hybrid force to protect undersea infrastructure from Russia. Norway will be joining Atlantic Bastion as well, and the Royal Navy is looking for other allies to join.[82]

The January 2026 Hamburg Declaration, signed at the North Sea Summit, included several landmark commitments to collaboration, including a commitment to building up to 100 GW of joint offshore wind in the North Sea and connecting electricity grids across borders. Critically, it also included commitments to 'take coordinated and decisive steps' to increase the security of offshore infrastructure through coordination and collaboration, and calls on energy and defence ministers to lead this charge.[83] In pursuit of the 100 GW commitment, the North Sea States, wind industry (represented by WindEurope), and Transmission System Operators (TSOs) also signed the Joint Offshore Wind Investment Pact for the North Seas, establishing clear commitments to build, de-risk, reduce costs and create jobs in the North Sea.[84]

While these efforts are critical, they are relatively disparate and, so far, include more goodwill than concrete implementation.

Figure 4: Comparison of gas storage capacity in the UK and other countries



The lens of energy security shows how we can use the energy transition to make the UK more secure as we transition away from gas

As the Ukrainian experience demonstrates, the decentralised nature of renewable energy makes it highly resilient but, paradoxically, the speed with which electricity moves also removes a buffer that gas provides. For decades we have relied on the fact that gas flows slowly as part of our resilience planning – even if new inputs cease, we have a few days of grace to sort out the situation. As we transition to a new normal, our ambition should be to combine the strengths of the legacy and clean systems and increase our resilience to attacks.

Throughout the workshop, it was noted that the UK's gas storage, while much lower than other European countries'[85], is a key tool in the case of a crisis. In the pipeline explosion scenario, gas storage would act as a buffer, allowing time for market incentives to step in and make up for lost supply. In a diversified energy mix, long duration energy storage (LDES) can and should play a similar role in increasing our resilience to system shocks. Renewables are often associated with intermittency rather than stability – but increasing our deployment of LDES (be it batteries, hydro, hydrogen or novel technologies) will mirror the system stability provided by gas – whilst also allowing it to be more widely distributed and secure.

And as the UK continues to struggle with a high cost of living and tight fiscal constraints, zero marginal cost energy can act as inflation-proofing. The UK's reliance on gas to maintain grid stability leaves us vulnerable to the price volatility of the international gas market, which still sets the price of most of the UK's electricity. When there is strain anywhere in the market, UK consumers feel the impacts.

Renewable energy, however, is a domestic energy source with little-to-no marginal cost. If enough is built to meet UK demand and reduce our reliance on imported oil and gas, UK energy bills could lower significantly. Given the declining role of the North Sea, renewables can step in as an alternative source of secure domestic production.

In conclusion: reinventing energy security

5.

The UK has one of the most secure electricity systems in the world[86] but this has come at a cost. NESO keeps enough generation on standby to cope with the instantaneous loss of the biggest asset on the system, and renewable energy has allowed a significant number of smaller assets onto the grid that can reduce the cost of these redundancies. However, around 30% of our electricity still relies on gas, leaving us critically vulnerable to price spikes due to state and non-state aggressors, bad weather, market fluctuations, and the whims of unreliable allies in an increasingly lawless international order.

We cannot provide redundancy for 30% of our electricity system so we are forced to simply pay whatever the going rate may be. Essentially, even as we reap the benefits of increasing decentralisation, we remain tied to a fuel for which the insurance policy is to simply pay more. That downside risk is heightened by a market structure which means that gas sets the price of our electricity most of the time (85% of time periods in 2024[87]).

Meanwhile, the high cost of electricity has become an increasingly political topic, and is a key factor in decreasing the output of our energy-intensive industries – which is at the lowest level since the ONS began recording in 1990.[88] And the British public is becoming increasingly impatient with Governments that claim they cannot afford to make substantive change. Taking dramatic action is hard but a lack of change is eroding trust in Government. This is a dynamic that our enemies – whoever they may be – can exploit. There is no need to start a costly war with the UK when repeated gas prices shocks will bring us to our knees just as effectively.

There are better ways to achieve energy security. New technology developed over the past few decades has allowed electricity generation assets to become smaller and more distributed. This means that losing one is far less troublesome for the grid, and a big emergency is harder to create.

Nonetheless, it remains true that our commitment to redundancy in the system results in additional costs, passed onto consumers through energy bills. We keep generation ready and waiting so that an interruption of almost any size can be smoothly handled by the system without any consumers noticing. This approach does too little to leverage the new tools available to us via both demand flexibility and long duration energy storage.

For too long energy security debates have been stuck in an unproductive stand-off between the fossil-fuel proponents who are wary of variable renewables, and the clean energy advocates focussed on a renewable future. As we showed in chapter one, the energy transition is upon us – to resist it is to make the UK even more vulnerable to gas market fluctuations and the whims of our enemies. What is needed

now is a clear-headed view of the benefits our old system offered and how we can achieve those in the new world, accompanied by a willingness to embrace the innovative tools available now that policymakers of the 1970s would have been thrilled to get their hands on.

Combining the strengths of our legacy and new energy systems to withstand the challenges of this uncertain era will require redefining what 'business as usual' looks like in our energy system. The focus of policy needs to shift so that it provides whole of society protection – protection of our national budget included. Doing that requires accepting that business as usual at any cost is no longer a viable goal. Instead, we must harness the features of newer technologies to make demand more flexible and resilient to shocks to the system. This will allow both renewables and oil and gas to respond to crises more effectively, while shielding business and consumers from the economic consequences. This can be further supported by improved communication and information sharing both within and across our legacy and new energy systems.

This is no small ambition. As Government prepares to publish its Energy Security and Resilience Strategy, we draw out six key recommendations for Government to make this ambition a reality. Each one alone would merit multiple reports, but we offer here a strategic direction.

Integrate citizens and business into a whole of society approach to energy by encouraging participation in energy flexibility

By definition, a whole of society approach to defence and to energy in the UK must integrate citizens and business. Most people tend to be relatively detached from the realities of defence and energy systems. However, to build a resilient system, we need to show how the intermittency and flexibility of renewable energies are a feature, not a bug. Sometimes we will have more energy than we can use – given the right framework, this abundance acts as an incentive for households and businesses to install smart tech that can soak up cheap, excess power. Conversely, it allows for greater flexibility in use if we face restrictions due to an attack on our generation or transmission infrastructure. Supporting electrification and access to flexibility is a positive both for consumers and for resilience and must be a continued priority for UK Governments.

Additionally, a focused recruitment drive to bring companies into demand response mechanisms of one kind or another is vital. As part of this, regulatory change will be required to make it easier for more businesses – and potentially communities – to take advantage of new technologies and install generation and storage behind the meter. This will reduce energy bills (which remain perilously high) and demand for grid connection upgrades (also at an unserviceable level) while increasing both the resilience of those businesses and the nation in the event of an attack on our energy supply.

Whole of society resilience must include energy – and energy spending

Energy must be clearly and explicitly integrated into UK resilience strategies. It is a vital resource that cannot be taken for granted, in both our defence and across wider society. This is becoming especially apparent given the explicit and frequent targeting of energy assets by Russian grey zone attacks.

NATO allies have committed to spending 5% of GDP on defence in order to increase their contributions to collective security and reduce reliance on the US. At least 1.5% of this expenditure must be allocated to 'protect critical infrastructure, defend networks, ensure civil preparedness and resilience, innovate, and strengthen the defence industrial base.'[89] There is not yet a clear guiding framework for meeting this portion of the commitment.

The UK should therefore take the lead and work with NATO to develop a framework by which spending on energy system resilience can be accounted under the 1.5% target. This has been previously called for by a group of retired senior military personnel, who argued that 'to have a strong military deterrence, we need a resilient homeland', and that renewable energy is a key factor in that resilience.[90] This broader understanding of our security is necessary in a world that has largely moved past traditional, isolated land wars. While this spending should be considered as a critical *additional* aspect of our defence spending, rather than as a replacement for existing commitments from Government, it would also make it easier to reach our 5% target, which could have positive implications for the UK's relationship with the US. To further integrate energy into defence, new energy infrastructure could co-locate near military installations, and they could have first access to any power being generated.

Deepen international collaboration to protect critical undersea energy infrastructure in the North Sea

The security of all North Sea nations depends on the ability of each to defend the region's critical infrastructure, and collaboration is the most effective way to strengthen that capability. Given the tangible current threat posed by anchor dragging, energy installations should have multiple points of connection. This is a potentially costly enterprise but one that will reduce the ability of small, unattributed attacks to affect energy generation. One way of managing the risk and reducing the cost of such a plan is to collaborate across companies and countries to create an energy grid in the North Sea. Some work on this is already underway but the UK remains on the periphery due the after-effects of Brexit.

The January 2026 Hamburg Declaration included several commitments to collaboration, including building up to 100 GW of joint offshore wind in the North Sea and connecting electricity grids across borders. Critically, it also included commitments to 'take coordinated and decisive steps' to increase the security of offshore infrastructure through coordination and collaboration and calls on energy and defence ministers to lead this charge.[91] This is important work that must not be delayed. As recently recommended by E3G, a leaders-level 'sherpa group' should be established to drive decision-making and delivery.[92] This also creates an opportunity for the UK to step up and be a regional leader in the push for a secure North Sea. Commentators have suggested that the UK should volunteer to hold the next meeting of the group, and we agree that this would be a proactive and sensible step forward.

Reconfigure the nation's strategic reserves for a new era

A critical aspect of resilience is ensuring that we can respond and recover, both at military and civilian levels, as quickly as possible. As the energy transition proceeds, the types of reserves held by the nation will need to evolve. That means a renewed focus on gas storage, long duration energy storage for electricity, and spare parts for our fundamental transmission networks.

Maintain gas storage

Gas remains an important fuel in the nation's energy mix and crisis planning makes substantial use of the fact that gas is a physical substance that takes time to flow through pipes and can be stored. These physical attributes currently give us around a week of buffer time to resolve supply constraints. However, behind these reassuring timelines is an asset base of pipelines and storage sites that require upkeep and security. As our use of gas as a fuel to create electricity reduces over time, we are already seeing the reduction of interconnector capacity, and the temptation may be to also reduce our domestic storage capacity. This would be a mistake. Counterintuitively, as gas use declines, storage as a multiple of daily use must be allowed to rise in order to insure against increasing volatility in both our usage and geopolitical context.

Increase LDES to mirror our historic storage of oil and gas

We should be working towards achieving greater levels of Long Duration Energy Storage (LDES), much as we have historically stockpiled fuel oil and coal. More LDES can drive down the costs of electricity across Great Britain while also providing energy resources for our armed forces in the event of a crisis. A thriving commercial battery sector is crucial to underpin the day-to-day energy market, and the military should explore procuring further, inter-seasonal storage as part of its own investments in energy infrastructure delivery. Such energy reserves could be co-located with military facilities - or built on other resilient sites – and used to prolong our resilience in the event of a gas shortage or price-spike, to aid in restarting the grid after an incident, and even to power our military response in the event of need. This will also complement the LDES solutions that are coming to market already via mechanisms like the cap and floor and the Capacity Market.

Create reserves of physical hardware required by our energy system

The best way we can demonstrate the resilience of our energy system to those adversaries who may wish to target infrastructure is to show how quickly we can fix things. The availability of spare parts emerged as a potential barrier to fast repair in our gas pipeline explosion scenario. Individual asset owners will have their own procedures in place but given the extent to which the nation relies on the flow of gas and electricity, it is proportionate for the state to also monitor this. Government could regulate to ensure that operators keep spare parts available and in-country or, potentially, hold a national reserve of items including cables, transformer parts and mobile substations for use in emergency situations. Either solution would be most effective when underpinned by an agreed-upon standardisation of certain equipment to facilitate increased production and stockpiling.

Draw renewable energy into existing security channels to adapt to new threats and technologies

Industry and Government regularly rehearse for a gas emergency, so emergency procedures are clear. However, the relative robustness and decentralised nature of our renewables sector means that equivalent emergency procedures have not yet fully developed; good practice exists in some areas but must continue to develop and spread. Working together, Government, the energy industry and the MoD must collaborate to protocolise these procedures in order to increase and maintain the security of renewable infrastructure.

One of the consistent blockers to effective collaboration is a lack of clarity over which aspects of security sit with the renewables industry, and which sit with Government. Protocolisation must therefore begin with a clear, agreed-upon delineation of responsibilities and costs.

Government and industry must then urgently work together to adapt existing emergency response systems and further draw in renewables. This could be achieved through existing bodies – such as the Energy Resilience Forum - with the goal of establishing clearer processes through which renewable energy operators notify NESO, MoD and DESNZ in the case of emergency. Among other goals, this collaboration could:

- Increase the speed with which incidents are made known to the wider industry and Government so that wider contagion can be avoided (as per our case study of Baltic security networks – see page 14);
- Inform investment in cyber and physical security features; and
- Improve the speed of recovery in the event of an attack by ensuring that communications channels are well known and operate smoothly.

As well as drawing renewables more firmly into existing systems of communications, threat surveillance and information sharing should be improved to better capture data on the growing cyber threat. This must include more compulsory, detailed reporting of cyberattacks to allow for improved cross-sector coordination, but could also be expanded to include, for example, shared data from integrated intrusion-detection sensors on offshore installations. Without further investment in this capability, neither the boards of energy companies, nor Government can make informed judgements about how to invest in future resilience.

Consistency and clarity are key here; for example, anecdotal data from the sector suggests that there is inconsistency in the manner in which Ofgem is currently applying the 2GW threshold, and whether it applies to whole sites or sub-projects within them.

Re-evaluate the thresholds for strategic assets to account for new, distributed threat vectors.

A key aspect of drawing new energy infrastructure into existing security channels is adapting those channels to accommodate the decentralised nature of renewables. Decentralisation is a strength because, as we realised in designing our crisis scenarios, it makes it much more difficult to attack a significant amount of generation at once. However, the December 2025 co-ordinated cyberattacks on more than 30 Polish energy assets[93] revealed that lower security standards at decentralised sites can still present a risk of wider system failures if multiple sites are attacked at once. This tactic relies on a corollary of the system by which we choose which assets are more important to protect (largely based on size): hackers attacked the smallest units but those could have been defended better.

Russia has proven its ability to mobilise a significant number of hackers, using relatively unsophisticated means, to inflict damage on the system. Now the UK needs to adapt to this threat by adapting the size thresholds for strategic assets to account for distributed threat vectors. While it would not be a critical loss to the system if one wind farm was attacked, a successful attack on 30 has the potential to cause severe disruption.

Currently, some smaller UK energy generators sit below the threshold for cyber security risk management requirements set by the Ofgem and DESNZ because they produce less than 2GW of electricity – and the system is therefore able to cope with the loss of the asset with relatively little impact. This threshold must be reassessed in light of the changing threat. While it is very unlikely that even a lower threshold would bring all generators into scope of far tighter statutory regulation, the Alan Turing Institute has recommended that all industries related to the offshore wind sector should develop and implement further cyber security processes modelled on the pre-existing the ISA/IEC 62443 International Standard, which should also be subject to an audit regime.[94]

Endnotes

1 Davos 2026: Special address by Mark Carney, Prime Minister of Canada
2 As Oil Tankers Come Under Attack, Experts Fear for Global Trade Through Strait of Hormuz
3 Maps and charts of the Iran crisis
4 Trends in UK imports and exports of fuels
5 Leading natural gas exporting countries in 2024, by export type
6 The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure
7 Russia is 'exporting chaos', new head of Britain's spy agency MI6 warns
8 The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure 3
9 Russia's 'disposable' saboteurs spread chaos across Europe
10 Cyberattacks during the Russian invasion of Ukraine
11 'Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says
12 China's 'accidental' damage to Baltic pipeline viewed with suspicion
13 Supporting Ukraine: The Fight for Light
14 Miles-long anchor drag mark found on Baltic seabed after suspicious cable damage, Finnish investigators say
15 How serious is the Russian spy ship move?
16 Navigating the grey zone: Readiness, solidarity and resolve
17 Cost of the fossil fuel crisis in the UK - November 2025
18 Is there a £22bn 'black hole' in the UK's public finances?
19 Constituency data: Central heating
20 What has led to France's u-turn over gas boiler ban?
21 The fall of UK North Sea oil and rise of offshore wind
22 A history of natural gas in the UK
23 Comment: North Sea oil and gas
24 How much shale gas is there in the UK and what is the status of fracking?
25 Trends in trade of Liquefied Natural Gas in the UK and Europe
26 Davos 2026: Special address by Mark Carney, Prime Minister of Canada
27 The energy leap: How EU countries weathered a Russia-induced crisis and are reshaping energy supply
28 Cost of the fossil fuel crisis in the UK - November 2025
29 Chief of the Defence Staff speech - 15 December 2025
30 The UK Government Resilience Action Plan: The UK's strategic approach to resilience
31 Defence Industrial Strategy: Making Defence an Engine for Growth
32 Strategic Defence Review 2025 – Making Britain Safer: secure at home, strong abroad
33 Prepare Campaign
34 Nordic-Baltic total defence: easier said than done
35 Security Strategy for Society: Vital Functions of Society
36 Nordic-Baltic total defence: easier said than done
37 Security Strategy for Society
38 This is civil defence
39 Civil defence objective
40 Sweden: reinventing total defence and a proactive stance in NATO
41 Defence Resolution 2025-2030
42 Defence Resolution 2025-2030
43 ERCOT increasingly meets rising demand with solar, wind, and batteries
44 ERCOT increasingly meets rising demand with solar, wind, and batteries
45 Supporting Ukraine: The Fight for Light
46 Ukraine built more onshore wind turbines in past year than England
47 The wins of COP that nobody noticed
48 Lessons learned from Ukraine's fight for light
49 Lessons learned from Ukraine's fight for light
50 DTEK to invest €450 million to expand Tyligulska windfarm in largest investment since war in Ukraine began
51 Powering Ukraine: DTEK and Octopus Energy Group launch RISE initiative to boost energy resilience
52 DTEK raises UAH 3 billion (€67 million) from consortium of banks to build one of the largest energy storage complexes in Eastern Europe
53 Baltic Sea Cooperation
54 Civil Security
55 Finland investigates outage of undersea power link to Estonia, Finnish PM says
56 Sixty-mile drag mark found near damaged Baltic Sea cable, says Finland
57 National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK
58 Code of practice for property flood resilience (C790)
59 Property Flood Resilience (PFR): Things to Consider
60 Flood Resilience 10 Top Tips: Preparing for and Responding to UK Flooding
61 National Risk Register - 2025 edition
62 Gas system in transition: security of supply - 2025 UK Government consultation
63 Britain on gas alert as extreme cold freezes Norway's undersea pipelines
64 The Texas Big Freeze
65 How changing weather patterns are affecting UK wildlife
66 Energy Sector Incident Report - 29 December 2025
67 Three men found guilty of Wagner-linked arson attack in London
68 Demand Flexibility Service explained
69 Net zero target threatened as popularity of electricity rationing scheme collapses
70 Electricity Engineering Standards Review: Independent Panel Report 72
71 Army hails first solar installation as part of Project PROMETHEUS
72 DE&S estates to become carbon neutral by 2025
73 Strategic Defence Review 2025 – Making Britain Safer: secure at home, strong abroad 135
74 Defence Industrial Strategy: Making Defence an Engine for Growth 69
75 Great British Energy to extend solar scheme to military sites
76 Clean energy upgrades for hospitals and military sites
77 MOD Land Holdings: 2000 to 2024
78 Long-Duration Energy Storage
79 Lockheed Martin earns military stripes with 8.5MWh cost-saving Fort Carson project
80 Boosting renewable energy for Defence in the north
81 UK and Norway to operate together to counter Russian undersea threat through major new defence agreement
82 First Sea Lord's speech to the International Sea Power Conference
83 The Hamburg Declaration: Building the North Seas' power hub for a resilient and competitive Europe
84 Joint Offshore Wind Investment Pact for the North Seas
85 The role of gas storage in ensuring energy security
86 National Electricity Transmission System Performance Report 2024-25
87 Analysis: Growth in British renewables cutting electricity prices by up to a quarter
88 The impact of higher energy costs on UK businesses: 2021 to 2024
89 Defence expenditures and NATO's 5% commitment
90 Renewable energy investment should come from defence budgets, say retired military leaders
91 The Hamburg Declaration: Building the North Seas' power hub for a resilient and competitive Europe
92 Empowering Europe: Delivering the security and economic benefits of clean energy in the North Seas
93 Energy Sector Incident Report - 29 December 2025
94 Enhancing the Cyber Resilience of Offshore Wind

RenewableUK
6 Langley Street
London
WC2H 9JA
United Kingdom

T: +44 (0)20 7901 3000
E: info@renewableuk.com