

RAND EUROPE

Expert Insights
PERSPECTIVE ON A TIMELY POLICY ISSUE

JAMES BLACK, KIRAN SUMAN-CHAUHAN, LEANNE IORIO
CONTRIBUTORS: STUART DEE, JACOB PARAKILAS, HENRI VAN SOEST, ALEIX NADAL CAMPOS, JUDITH HUISMANS, TARA ZAMMIT, MATTIAS EKEN, ARTUR HONICH, SONJA MARJANOVIC, MEHDI SHIVA

Ready for war 2030: a scenario

Bolstering the UK and NATO's preparedness

NOVEMBER 2026

THIS WORK WAS MADE POSSIBLE BY RAND'S OWN RESOURCES, INCLUDING INCOME FROM OPERATIONS, UNRESTRICTED GIFTS FROM RAND SUPPORTERS, AND DISTRIBUTIONS FROM ITS LONG-TERM INVESTMENT FUND.

RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis.

Limited Print and Electronic Distribution Rights
This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html.

Cover image: UK MOD © Crown copyright 2026

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

For more information on this publication, visit www.rand.org/t/PEA5505-1.

© 2026 RAND Corporation

1. Context of this RAND paper

1.1. Though conflict is certainly not inevitable, there is a growing risk that NATO finds itself in a defensive war against Russia by 2030

Russia continues to wage its war of aggression in Ukraine and has stepped up its subthreshold operations against the UK and its NATO Allies in recent months – from cyberattacks, sabotage of defence and critical industries, and disruption of Alliance airspace and communications. Threat assessments and warnings from NATO, the EU and national governments suggest there is now a credible threat of peer-level war in Europe by 2030. With Europe committing to military rearmament and investing to bolster readiness and resilience, it is no longer a question of whether a war is feasible, but whether we will be prepared to meet the challenge.

While this may at some point include open, high-intensity warfare, it is expected that Russia would present threats across the full spectrum of competition, crisis and conflict. This includes everything from hybrid activity (of the kinds Europe is experiencing today) in supposed peacetime and the 'transition-to-war' phase, up to conventional warfighting and – in the most extreme scenarios – various forms of nuclear escalation. Indeed, recent RAND research indicates that from a Russian perspective, conventional warfighting would be an extension of what they perceive as on ongoing strategic confrontation with NATO.[1] The UK and its NATO Allies need to be prepared to handle this array of threats – and crucially, to do so without relying as heavily on the military and industrial contributions of the United States, which has underpinned Euro–Atlantic security since the Second World War but which is now likely to be taking the lead in other regions.

1.2. Defence budgets are increasing, if more slowly in the UK than wider NATO, but preparing for war also entails a profound mindset shift

After decades of low defence spending since the end of the Cold War – the so-called peace dividend – the UK armed forces are at their smallest size of the modern era. Further, the UK's current force mix is heavily weighted towards exquisite capability and precision at the expense of mass, a structure designed for the limited wars of choice fought by previous generations, rather than the peer-level conflict close to home that analysts are now expecting. Observations from the ongoing war in Ukraine have exposed trends in modern warfare in which the UK and NATO Allies are lagging behind, most crucially rapid innovation cycles, uncrewed systems and the rising value of cheap mass.[2] New operating concepts such as the Hybrid Navy demonstrate recognition of these problems– but this is not the same as being prepared for them, yet.

This is not to say that exquisite capability is not important or valuable. It remains a central pillar of modern warfare. Yet even on this front, the UK faces platform availability and maintenance issues, pressures on its training and exercise pipeline, shortfalls in munitions stockpiles, and overall readiness challenges.

Meanwhile, even outside of a traditional conventional war, the UK and NATO remain exposed in key subthreshold areas where malicious actors, including Russia, seek to

exploit ambiguity, deniability and the seams that frustrate responses from democratic societies. In particular, digital networks and critical national infrastructure (CNI) (e.g. underwater cables, energy grids, or transport, food and health systems) present a large potential attack surface for cyberattacks, physical sabotage and other hostile activity that sits below the traditional threshold of open war. Ultimately, then, greater effort is needed across the full spectrum of competition, crisis and conflict to ensure preparedness for a future war – and thereby deter one.

1.3. RAND Europe has developed a hypothetical scenario for 2030 through which to analyse intensifying threats and potential solutions

In this context, RAND has developed an illustrative scenario through which to present and analyse 12 vignettes exploring different potential dimensions to a future NATO–Russia war and how threats might directly affect the UK's security, economy and society. The authors draw out the broader problems in these spaces represented by each vignette and consider potential steps to prevent and mitigate them.

This scenario is not a prediction of events out to 2030 and beyond. Rather, it is one possible pathway that provides a tool through which to analyse the range of problems the UK and NATO Allies might face in the near future if our deterrence of Russia fails or if a crisis inadvertently escalates into full-blown conflict. It is in places deliberately provocative to draw out these issues, but readers should keep in mind that the scenario remains an illustrative framework for wider analysis rather than a comprehensive or predictive instrument.

The baseline scenario is set out below in Box 1. Each vignette explores aspects of the envisaged war at different points in the scenario timeline, allowing for chronological as well as topical analysis.



Algimantas - Adobe Stock

Box 1: RAND Europe's illustrative scenario for war in Europe in 2030

January–March 2027: the death of Putin and a Russian succession struggle

In January 2027, the Russian president dies of natural causes. In the power vacuum he leaves behind, there is no clear successor, and the disparate elements of the Russian state apparatus vie for power. The Russian security services emerge as the victors of this power struggle, and in March, the Kremlin announces a former Federal Security Service (FSB) general as Putin's formal successor as President of the Russian Federation.

April 2027: ceasefire in Ukraine

The new Russian president immediately looks to shore up domestic authority and reconstitute the Russian political system around him as a first priority. Since neither side has been able to achieve a decisive breakthrough in Ukraine, the Russian president therefore agrees to a ceasefire negotiated by the United States and supported by the UK and other major European states, including partial sanctions relief.

July 2027: formal peace negotiations stall

Although negotiations for a formal peace treaty stall – since Russia's underlying war objectives have not fundamentally changed – in practice, the war in Ukraine devolves into a frozen conflict. There is no large-scale fighting on the front, but the Russian Federation maintains its claim to occupied Ukrainian territory and has holding forces continuously deployed there. Without the need to maintain a large-scale offensive in Ukraine, the Russian president subsequently directs the Russian armed forces to turn their attention to reconstitution.

January 2028 onwards: hybrid campaign against NATO

By January 2028, the new Russian president has begun to replace some of Putin's closest allies within the Kremlin's power structures with subordinates whose personal loyalty is more assured. However, with both a struggling economy and the long-term societal impact of military losses from Ukraine, there is continued domestic unrest among both the public and elites. The result is that he is still far from secure in power and has yet to replicate Putin's dominance over the entire system. In particular, military hardliners advocating for harsher measures against NATO are seen as potential threats with dangerous power bases.

As an internal display of authority and intent, the Russian president therefore directs the organisation of a targeted campaign of hybrid activity against NATO Europe. The UK, alongside NATO Allies across Europe, begins to experience intensifying, difficult-to-attribute disruptions across their respective societies, including interference with communications

networks, energy infrastructure and other CNI, and key industry players. In Eastern Europe, disinformation narratives ramp up around mistreatment and discrimination toward ethnic Russian minority populations, while in Western European states these narratives focus on exacerbating divisions between Allies bilaterally, supporting separatism, and fomenting resentment of multilateral institutions. Public rhetoric varies around explicit attribution towards Russia, with Eastern Allies taking a more hardline approach and Western states typically behaving more cautiously. Although European NATO Allies recognise the need to build whole-of-society resilience, progress is generally slow, inconsistent and uncoordinated.

June 2029: the South American crisis

Meanwhile, a crisis in South America sparks a wave of conflict and violence on the continent. The US administration makes it clear that this crisis is its national security priority, continuing the trend of retrenchment from Europe in favour of bolstering the US military presence and posture in other theatres. The UK and other European Allies plan on the assumption that they may receive logistical and strategic support from the United States but do not expect large numbers of additional US platforms and personnel to be deployed to Europe until such time as the South American crisis is resolved, especially given enduring tensions with China in the Indo-Pacific.

January–April 2030: the transition to conflict

By 2029, sustained pressure from the military elites has forced the Russian president's hand, and, encouraged by the United States' apparent preoccupation in other theatres, the Kremlin is directed to develop a plan for an intensified hybrid campaign and limited military action in the Baltic States, focusing on areas with a higher density of ethnic Russian populations. The intent is not territorial acquisition but rather to demonstrate that NATO does not have the unity nor the will to defend Eastern Europe, thus driving a permanent wedge between the Allies by proving that Article 5 of the North Atlantic Treaty does not credibly result in collective defence.

Hybrid activity across Europe escalates sharply to prepare the ground for the planned offensive. Incidents increase not just in quantity but also in severity – every hybrid attack is carefully calibrated to remain uncertain in attribution, while probing national preparedness (e.g. response times), testing and exposing vulnerabilities at key military or infrastructure sites, and overall weakening NATO's will to fight.

As the framework nation for both the Enhanced Forward Presence (eFP) in Estonia – part of NATO Forward Land Forces – and for the Joint Expeditionary Force (JEF), Russia identifies the UK as one of a number of priority targets to address in order to slow the delivery of rapid military support to the Baltic States. Hybrid attacks are increasingly concentrated on UK military networks and enablers, including communications, the defence industry and transport networks. The goal of these attacks is not just to limit Allied ability to coordinate and contribute to an armed response to the Russian incursion but moreover to limit Western will to do so in a timely fashion in the first place.

May 2030: the outbreak of war

Russia exploits connections with ethnic Russian populations in Estonia to foment protests, which escalate into riots in the heavily Russian border city of Narva. The Estonian authorities react, cracking down with force on the rioters. The Russian president immediately responds by announcing that the Estonian government can no longer be trusted with the safety and security of the ethnic Russian population in Narva, thus requiring an intervention to allow for Russian state protection. On this claimed basis, the Russian armed forces launch a limited incursion across the Estonian border around Narva, with the aim of securing the city and immediate surrounding areas.

The Russian plan hinges on the assumption that European NATO Allies have demonstrated an aversion to conflict and a lack of willingness, and ability, to commit to war. The working Russian assumption is that Western European Allies are broadly willing to accept a limited incursion to avoid escalation into a full-scale conflict. The Russian president gambles that although the NATO response is likely to amount to an Article 5 declaration, the subsequent response will be insufficiently cohesive and unified and will thus fail to result in the Alliance mounting a full-scale military response – thus demonstrating fractures between Allies and undermining the principle of collective defence.

However, NATO immediately rallies around Estonia, responding not only with a rapid declaration of Article 5 but also a commitment of most Allies (if with a limited role for the United States) to provide direct military support to the defence of Estonian territory and remove Russian forces.

June 2030–October 2030: full-scale warfighting

Surprised by their miscalculation, Russian forces quickly pivot towards posing strategic dilemmas to NATO in a bid to force them into a decision between cutting their losses or committing to a peer-level conflict on the back foot. This includes the expansion of the conflict into the High North, with threats to Svalbard and Northern Norway and with the Russian submarine fleet attempting to break through into the North Atlantic.

The UK is seen as a priority target. Russia calculates that by knocking the UK out of the war early, the Greenland, Iceland, UK (GIUK) Gap and therefore the Atlantic could open up to Russian submarines, allowing them to threaten sea lines of communication (SLOCs). The UK is also explicitly targeted due to its importance in offering NATO strategic depth and flexibility – namely the ability to receive and stage reinforcements from across the Atlantic, and for the UK itself to deploy the Allied Rapid Response Corps (AARC) as one of two Strategic Reserves Corps available to NATO's Supreme Allied Commander Europe (SACEUR). Russia therefore launches sabotage efforts, cyber-attacks and air and missile strikes at the UK homeland, with initial targets including air bases, ports, radar sites and command nodes.

As Allied forces from across Europe move to reinforce the Baltic States – with the UK contributing a land brigade, F-35 and Typhoon squadrons, and deep-strike capabilities – large-scale warfighting ensues across the eastern flank.

Meanwhile, anti-submarine warfare (ASW) efforts continue in the High North, with the UK contributing a carrier strike group and its Type 26 frigates to the effort to protect North Atlantic SLOCs. While fighting is limited on the southern flank, with Russia deliberately avoiding antagonising Türkiye – which has taken a back seat – the conflict still affects the region with both cyber and limited kinetic attacks affecting Southern and South-Eastern Europe.

November 2030: a tentative ceasefire

European NATO Allies hold the ground on NATO's eastern flank, preventing a Russian fait accompli but locking them into a war of attrition with no clear end in sight. Europe, including the UK, is struggling to sustain its forces after months of intense, full-scale warfighting, and the will to fight is waning.

Meanwhile, the Russian president faces internal pressures due to the political and societal fallout from failing to secure swift victory in Estonia. Building on the underlying tensions that remain from Russia's costly Ukraine war, he calculates that his position will soon become untenable if he cannot bring an end to large-scale warfighting and claim success both externally, in terms of the security of ethnic Russian communities, and internally, regarding his objective to undermine Article 5 credibility and fracture NATO.

With Russian forces occupying Narva and the majority of Ida-Viru County, he therefore announces that success in Russia's publicly stated objective – protection of ethnically Russian communities in the region – has been achieved. Before NATO forces can organise a counteroffensive, the Russian president proposes a ceasefire with European Allies, with the intention of forcing Estonia, which refuses to capitulate, into a practical inability to continue alone.

January 2031: an uncertain future

The ceasefire remains in effect as peace talks stall for months. Faced with the prospect of another frozen conflict and an increasingly destabilised Europe, NATO's credibility is damaged and the result is an uncertain and volatile security environment – leaving the future of European security in the balance.

2. Possible dimensions and challenges of war in 2030

This section analyses different aspects of wartime readiness in more detail via a series of illustrative vignettes. Each sets out a potential, indicative pathway that threats in each area might take through the progression of the scenario. The authors then explore what the broader problems are for the UK, and what the UK and likeminded NATO Allies can do to address the core issues affecting their preparedness for war by 2030.

2.1. Vignette 1: Managing threats to societal resilience

2028–2029

The UK intelligence community begins to monitor what appears to be a targeted disinformation campaign against disillusioned demographic groups in the UK, utilising AI-generated social media content tailored to individuals' public profiles. While its origin cannot be determined, the campaign's assessed objective is to exacerbate existing tensions, including narratives around illegal immigration, underinvestment in public services, and similar controversies. However, over time, elements of the narrative begin to coalesce around resentment of commitments to multilateral institutions and continued investment in defence spending at the expense of the UK's domestic institutions (e.g. the NHS), especially with the war in Ukraine being perceived as over.

January 2029

An operational failure at Grain Power Station in Kent and damage to power transformers in several other locations lead to blackouts across London and the southeast of England. Reporting on the exact nature of the failure is confused and vague, but authorities conclude that bringing the station safely back online could take several weeks. Some media outlets, citing anonymous industry sources, suggest sabotage by an unknown party. Power is diverted from elsewhere in the National Grid, but blackouts continue intermittently until the power stations resume normal activity in mid-February. Local authorities/services are inundated with urgent demand for backup heating solutions, with most homes in the area unprepared to deal with long-term disruption to electricity in the middle of winter.

September 2029

In a coordinated set of cyberattacks on the Tesco supermarket chain – the largest in the UK, holding nearly 30% of the UK's grocery market share – hackers gain access to the company's central systems and deploy encrypted malware, leading to the shutdown of systems throughout the distribution chain. Without access to automated warehouse management software or transport management systems, there is insufficient latent capacity in the workforce to make up for the loss manually. Within days, local depots are exhausted and shelves are bare. Media reporting and social media narratives around the cyberattacks suggest that shortages will last for weeks, if not months, leading to a wave of panic purchasing, creating even more chaos and disrupting attempts to manage food shortages.

January–April 2030

As the hybrid campaign against Europe intensifies, the UK begins to experience power outages and food and water shortages on a more regular basis as CNI disruptions from cyberattacks and suspected sabotage increase in frequency. Events escalate when some of the UK's critical undersea infrastructure (CUI), including submarine cables and energy interconnectors, are damaged. This disrupts data transmission for a fortnight before most capacity is restored, with full normal service not resumed until June. However, the damage is done in the first few weeks. Prolonged outage over several days leads to accumulating costs for energy providers and financial services.

Meanwhile, narratives propagated on social media shift towards pinning blame on the UK government, claiming there is no attributable 'enemy' disrupting UK society. Anonymous accounts continuously post falsified 'evidence' that the UK government is dealing with energy shortages by knowingly cutting power to already-disadvantaged areas, and that banks are manipulating the economy and secretly retaining vast profits. Protests pop up sporadically with increasing frequency, and in a few isolated instances, these escalate into civil disorder as panic and anger set in.

July–November 2030

As the war progresses and Russian strikes begin to target the UK homeland, the ports at Felixstowe, Southampton and Dover (among others) become priority targets. While the intent is to cripple the UK's strategic military transport capability (e.g. the Marchwood Sea Mounting Centre), the locations are also key nodes in the UK's CNI network.

The majority of the UK's sectors are impacted by the constraints on maritime traffic imposed by the war (including both damage to physical or network infrastructure at ports and also the threat posed by the Russian submarine fleet in the Atlantic and High North) – energy and fuel, food supplies, medical supplies, and even manufacturing industries all feel the pressure. Prices spike as a result, with rapid inflation even as ordinary citizens feel the tangible impacts of food and energy shortages and overwhelmed but undersupplied domestic services.

As the UK struggles to respond, Russia's online disinformation campaign shifts again to suggest that Estonia is the aggressor in the conflict and the UK government is subjecting its population to a costly war to defend a corrupt and unreliable ally. Small elements of the UK population seize upon this narrative and protests escalate to rioting.

2.1.1. What is the broader problem?

The UK military preparedness challenges are examined in detail below but equally concerning are shortfalls in societal resilience to withstand the implications of both hybrid and conventional attacks and the second- and third-order effects thereof. Although UK policy recognises this need for a whole-of-society approach to resilience, progress towards this goal has been slow and inconsistent. Like other NATO Allies, the UK remains vulnerable to threats like cyberattacks, sabotage, election interference and disinformation – vectors that the UK's adversaries can exploit while remaining below the threshold of war.

The problem is not a lack of ambition – indeed, the desire to move towards a more resilient UK has been articulated repeatedly and explicitly in recent policy, most prominently the Strategic Defence Review and UK Government Resilience Action Plan released in 2025.[3]

Where the UK currently falls short is the gap between this stated ambition and delivery on these objectives. The UK is relatively clear on what it wants to do but is still clarifying implementation priorities and timelines and investing from a low base. The government is developing a revitalised set of 'War Books' and a series of sub-strategies for critical sectors, such as an Energy Resilience Strategy, a Transport Resilience Strategy and a National Cyber Action Plan.

Reforms are already underway to enhance the emphasis on risk and resilience planning in policymaking, to bolster expertise in this area through a new UK Resilience Academy, and to improve the coherence of activity across government departments, devolved administrations and local authorities. Still, the UK is investing from a low base and full implementation of the Resilience Action Plan will mean overcoming political, financial, organisational, technical and cultural barriers. Though the government has launched a 'Be Ready' information campaign to bring resilience issues into focus, public awareness of threats and how to mitigate them remains low; it is also unclear what precisely NATO's investment target of spending 1.5% of GDP on resilience will mean in practice.[4] In short, the proposed 'national conversation' on resilience is at best only just beginning, and the UK continues to lag behind other societies with much more established preparedness mechanisms and more robust public dialogues around resilience.[5]

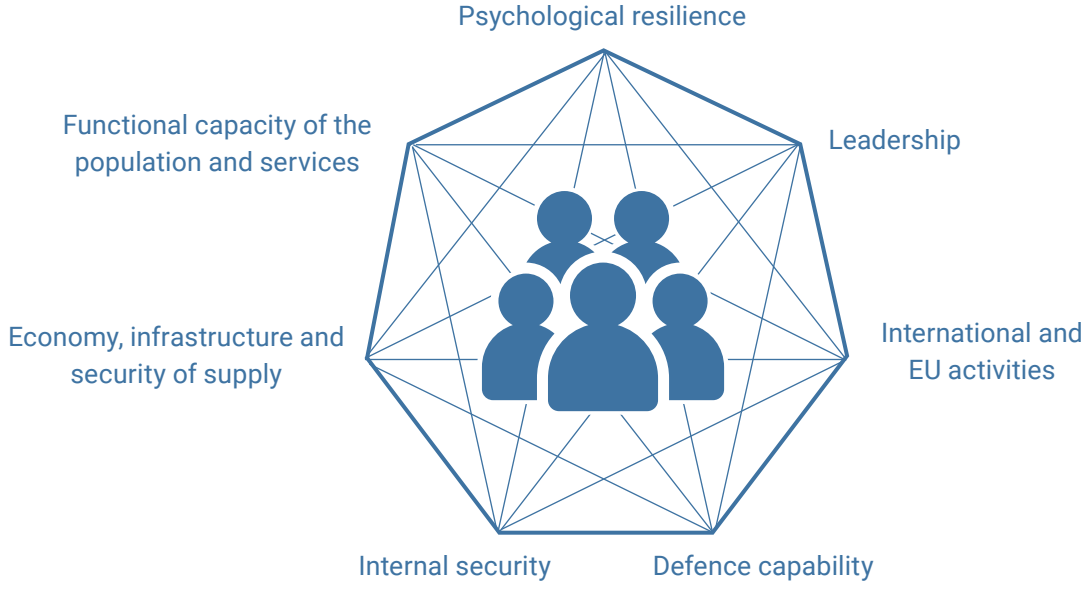
2.1.2. What can the UK do about it by 2030?

There are plenty of lessons that the UK can learn from allies and partners for whom national resilience has long been a priority. Indeed, in the Baltics, Nordics and Central European states, resilience and preparedness are

The UK is investing from a low base and full implementation of the Resilience Action Plan will mean overcoming political, financial, organisational, technical and cultural barriers.

embedded in the national consciousness to a far greater extent than with Western allies. Sweden, for example, calls its approach 'Total Defence', while Finland implements a 'comprehensive security concept' rooted in the safeguarding of seven 'vital functions for society' – of which defence capability is just one.[6]

Figure 1: Finland's Vital Functions of Society



SOURCE: Finnish Government (2025).

The UK can and should learn lessons from comprehensive security concepts to inform its own approach. These issues and lessons are further explored in RAND Europe's paper: *Strengthening UK national resilience and warfighting readiness: Pragmatic applications of Swedish Total Defence concepts and policies*. In this context, concrete steps towards generating resilience in the UK could include:

- **Develop a cohesive approach across government.** For example, the UK could assign a government department to lead resilience efforts, with binding authority rather than a convening role as is currently the norm. Combining this with a ring-fenced 'resilience budget' would offer unified political leadership and guidance to shape the UK's approach to resilience.

- **Improve civil-military coordination, integration and joint exercises to more clearly define roles and responsibilities, including for wartime.** This is required across government departments and needs to consider how roles might change across the full spectrum of conflict. Defence is no longer just responsible for warfighting but needs to be an engaged supporting actor in the pre-conflict phase too – for example, providing niche capability/resources for incident response that civilian bodies cannot afford to maintain.[7]
- **Strengthen trust at all levels.** This includes relationships and connections between not just Defence and other government departments but with the public too. Building awareness of threats like disinformation – as well as educating the public on how to address them, for example through understanding where to find reliable information, especially in a crisis – is crucial to mitigation. Generating trust also builds public confidence in the UK's ability to deal with hybrid threats, allowing the government to respond to and counter damaging false narratives as crises unfold.
- **Engage with the private sector.** The private sector will be important to any national response – for example, many CNI operators sit within this category (including energy companies, CUI services and financial services). Here, the UK could potentially learn from Sweden's approach, which mandates 'resilience statements' in annual accounts.[8] It could also involve routine exercises, not just cross-governmental but cross-sector as well, to nurture these relationships.[9] Crucially, engagement needs to go beyond voluntary industry participation to also consider levers by which government can incentivise or compel the private-sector to assist before, during or after a crisis; this means looking at everything from procurement contracts through to emergency legal powers.
- **Explore mechanisms for rapid cross-sector mobilisation of people and skills.** This could include partnerships with non-governmental organisations with pre-existing volunteer networks like the British Red Cross – these entities are often able to attract different demographics to directed government mobilisation.[10] Otherwise, the Reserves recall pool could potentially be expanded under the upcoming Armed Forces Bill and explicitly linked to a civilian 'war posting' concept, or existing ad hoc mechanisms like Military Aid to the Civil Authorities (MACA) could be formalised into a standing framework.[11]

2.2. Vignette 2: Mapping threats to supply chains in a war economy

January–April 2030

Defence Equipment & Support (DE&S) reports that MBDA UK, already operating with a significant backlog, has been unable to fulfil urgent orders of Storm Shadow and Aster missiles. The delays are due to an acute shortage in propellants for the missiles. By April, it is determined that the shortage originated with a small European company at the third tier of MBDA UK's supply chain providing the polymer binder for motor propellants to a Tier 2 subcontractor. The reason behind the shortage remains

unclear, but a Ministry of Defence (MOD) review concludes that the vulnerability – a clear single point of failure – was not captured in previous risk assessments. The polymer is marked as a critical material, but other European suppliers are difficult to find. The MOD is unable to take any further definitive action, leaving it up to MBDA to address the shortage.

May–November 2030

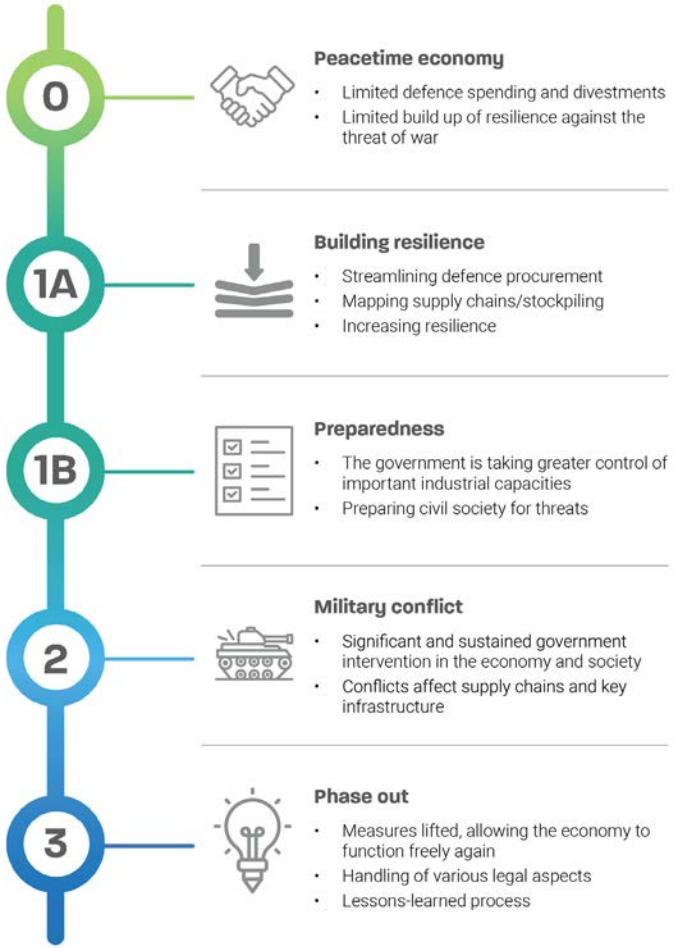
Upon the declaration of Article 5 and the outbreak of war, Parliament passes an Emergency Powers Act almost immediately. Building on the Civil Contingencies Act, this temporary legislation allows the MOD to issue priority directives to industries, requisition and allocate resources, and manage the workforce. However, in the initial weeks of conflict, the Act causes only confusion, with industry stakeholders expressing concerns over compensation amounts and timelines, and MOD employees unsure of how to utilise the mechanisms provided for and deconflict directives issued to industry internally. Although primes and sub-tier firms across many sectors express a desire to help and work with the MOD, some remain obstinate in their opposition until they receive clarity.

Meanwhile, the surge in production demand causes significant challenges as single points of failure are overwhelmed. Optimised for a 'just-in-time' procurement model, the majority of the UK industrial ecosystem struggles to obtain the sheer mass of critical raw materials and components it needs to scale up production – particularly as the war drags on and the impact of the conflict in terms of reducing UK imports and maritime traffic begins to manifest. Shortages in critical defence equipment, including complex weapons, conventional munitions, and spare parts for exquisite platforms soon begin to manifest, undermining the UK's ability to sustain combat operations.

2.2.1. What is the broader problem?

As set out in recent RAND work, a core element of national resilience is the ability to make an effective transition to a war economy, which allows a state to intervene in its economy and prioritise activity and production for defence and security purposes. In the context of the Russian war in Ukraine and growing hybrid threats, this is becoming an increasingly desirable option for European states. RAND Europe distinguishes between five distinct phases of a war economy – for the UK, despite an explicit ambition and recognised need to move to Stage 3 (Preparedness), concrete measures to do so remain limited.[12] Indeed, in some instances, as demonstrated by this and previous vignettes, the UK has arguably not yet fully fully implemented Stage 1A (Building Resilience).

Figure 2: Phases of a War Economy



SOURCE: Kreetz et al. (2025).

Industrial resilience is not yet fully embedded as a core objective in defence and security planning despite what may be stated in policy documents, with the current approach to crisis management reliant on emergency powers and goodwill 'making it work' in a crisis scenario. For example, although trust between government and industry is high at the prime level, for example, there is little to no coordination between government and Tier 3+ industry, with this largely taking place via primes if at all – in some cases, niche small- and medium-sized enterprises (SMEs) might even be unaware that their products eventually end up serving a purpose in Defence.[13] This makes Stage 1A (building resilience) difficult enough, let alone latter stages of shifting to a war economy.

Meanwhile, a core problem for the UK is a continued dependence on global supply chains for critical components across industries (e.g. semiconductor chips) and for raw materials (e.g. rare earth elements), increasing exposure to external shocks. Despite some progress, there is insufficient mapping and stockpiling of supply chain vulnerabilities and single points of failure, meaning that not only is the UK vulnerable to these shocks but may not even be aware of them – and therefore, would be unable to prepare for them.[14]

Nor is this solely an issue for advanced technological components such as semiconductors or critical raw materials – vulnerabilities exist across sectors such as manufacturing (particularly steel), energy (the UK is a net importer of diesel and jet fuel), agriculture (the UK imports a large amount of fertiliser from Europe, for example) and healthcare (a large proportion of the active pharmaceutical ingredients used by the UK are manufactured abroad, including in China, India, the United States, and European states).[15] Even if the UK were to shift towards a war economy, there

are broader issues in terms of global dependencies outside of UK control that will need to be addressed in the long term to allow the UK to reach Stage 1B, and Stage 2 if required.

2.2.2. What can the UK do about it by 2030?

The UK has the right strategic ambition to prepare its critical supply chains to move towards a war economy if needed, but embedding this into activity at the operational level will require more focused, concrete implementation. Specific steps could include:

- **Legislate predetermined powers for activation in a crisis.** The UK's system currently relies largely on goodwill and the strategic relationship between the MOD and industry primes to make it through a crisis, which are useful elements to have but not conducive to implementing Stages 1B or 2 of a war economy. This structure leaves unclear what powers the UK government would actually have in an emergency, as well as the mechanisms through which they would be wielded. Legislation clarifying how and when the government can compel industry and workforces in a crisis – for example, prioritisation of orders, or the allocation of materials, resources and workforce – and what compensation industry can expect in return could provide certainty across the ecosystem and remove the need to improvise under pressure. This would give the UK clarity on what shifting to a war economy would entail for defence industry and supply chains, enabling specific planning to support this on the part of both government and industry stakeholders.
- **Systematically map critical supply chains.** Generating insight into supply chains is the only way to identify vulnerabilities and single points of failure and to plan accordingly. This should involve not just mapping, but stress-testing and then strengthening where appropriate. Strategies to strengthen supply chains could include stockpiling strategies, supplier diversification, and onshoring or 'friend-shoring' critical industries, including with state intervention where necessary.
- **Coordinate bilaterally and multilaterally to develop joint capacity to build resilience to shocks and pressures.** Geographical realities mean that the UK can never completely overcome its reliance on international supply chains. However, the development of joint approaches and frameworks with NATO Allies and other partners towards issues such as labour supply management (e.g. right-to-work permits in specific sectors) or collaborative procurement (including both multinational defence projects and bespoke agreements on non-military imports and exports) would help bolster collective industrial and supply chain resilience.[16]

2.3. Vignette 3: Managing threats to critical national infrastructure

2028–2029

Throughout 2028 and 2029, UK and Allied maritime authorities observe growing incidents of vessels sailing slowly over or near undersea cables, pipelines and interconnectors and note a marked increase in ships drifting off course. Whilst not explicitly an illegal activity in international waters, the UK faces challenges in distinguishing

between legitimate maritime traffic and deliberate mapping for possible future sabotage. A joint Allied naval exercise near Svalbard detects and disrupts what appears to be a Russian exercise by the Main Directorate of Deep-Sea Research (GUGI), which operates specialised vessels capable of cutting deep-sea cable infrastructure. While the cable connectivity has yet to see major disruptions, the UK feels mounting pressure stemming from assessments of an increasingly mature Russian capability to conduct successful covert attacks on critical undersea infrastructure.

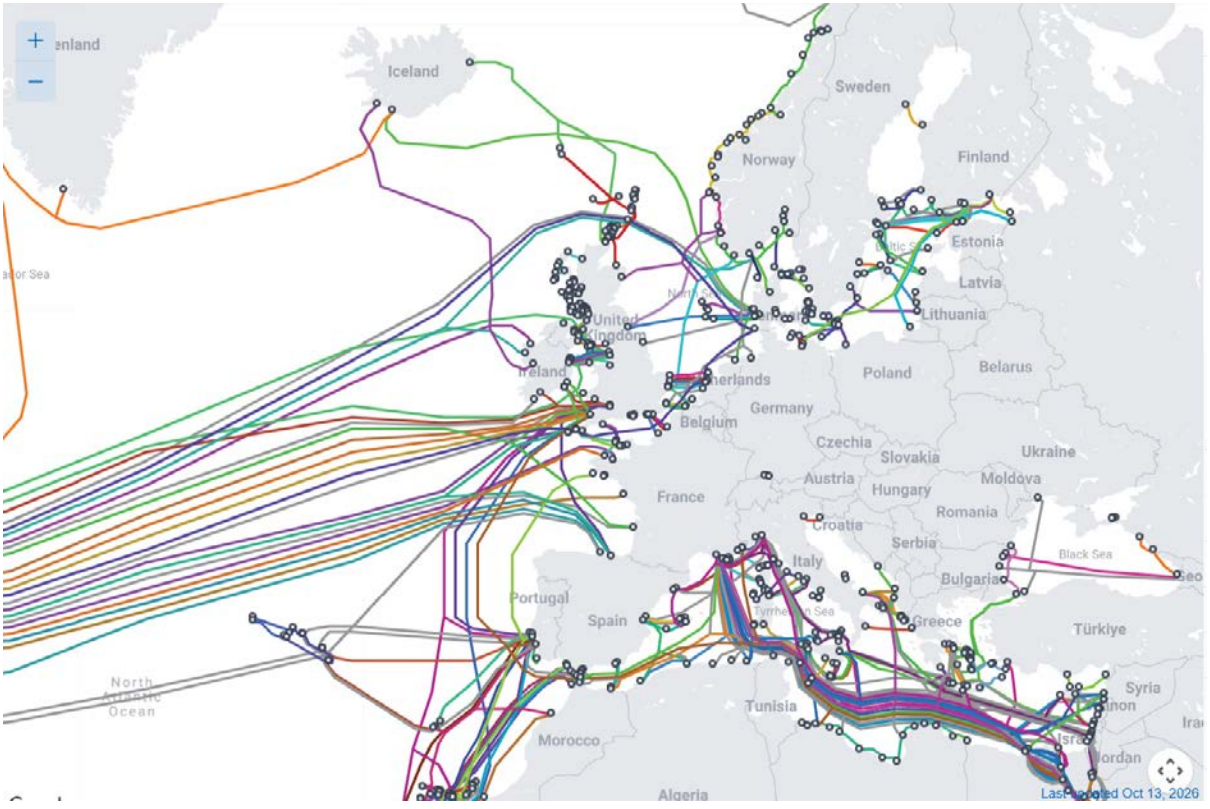
January–June 2030

Events come to a head in January 2030, when several of the UK's critical submarine cables are simultaneously disabled. It is unclear exactly how the damage occurred, but the presence of suspected Russian shadow fleet vessels in the vicinity of each incident leads the Royal Navy to assume a deliberate anchor-dragging incident or similar. The damage significantly disrupts data transmission for a fortnight before meaningful capacity is recovered, with full service not resumed until June due to a finite capacity of specialist ships and equipment required to repair and replace the damaged cables. However, the economic damage is done in the first few days, with billions of pounds of financial transactions between the UK, the United States and mainland Europe delayed or cancelled. Through mechanisms put in place after the 2008 financial crisis, such as enhanced capital requirements for banks, the crisis is contained before it becomes systemic. However, the delays to payment processing hinder commercial operations, leading to supply chain disruptions and leaving people unable to pay with payment cards or mobile phone wallets.

July–October 2030

Despite seeming resumption of connectivity via undersea cables in June, as the escalation to open war breaks out across Europe, the UK begins to experience an even greater uptick in major attacks on critical infrastructure over the following months. Russian shadow fleet vessels and GUGI deep-sea vessels conduct coordinated waves of attacks, which sees the IFA and IFA2 electricity interconnectors linking the UK and France being severed in August, taking offline critical power transmission capacity for at least eight weeks[17] alongside the simultaneous disabling of the Norway–UK Langeled gas pipeline. This leaves the UK with immediate-term localised blackouts and long-term difficulty in recovering the generation shortfall with a time horizon of many months[18] before gas pipeline repairs can be completed. Concurrent with the physical degradation of energy infrastructure, waves of targeted cyberattacks on the industrial control systems of energy companies lead to shutdowns of power stations for days at a time before control can be reinstated, further exacerbating the mounting energy crisis. The significant degradation of critical infrastructure succeeds in reducing the morale of the public and reducing the continued will to fight a full-scale war.

Figure 3: Undersea Cable Map, 2026



SOURCE: TeleGeography (2026). The coloured lines represent different cables, while the black circles represent landing sites.

2.3.1. What is the broader problem?

UK CNI and CUI remain highly vulnerable and under-protected relative to the threats faced, and even when the core elements of the infrastructure are protected, the second- and third-order elements are still susceptible to severe disruption and degradation. Some CNI and CUI assets are highly complex and specialised and have brittle supply chains. For example, electric power transformers, which convert electricity from high to low voltage and vice versa, are often custom-made, and replacements may take up to a year to arrive. Further, while undersea data cables have greater redundancies and shorter repair times, electricity interconnectors still lack a mature maintenance ecosystem and gas pipelines have close to no built-in redundancies.

This means not only that pipeline repair times can be six or more months but also that disruption to a pipeline connecting an oil or gas field to the mainland can result in the entire field being shut down and the pipeline becoming uneconomical to repair.[19] Europe's capacity to protect undersea infrastructure has not kept pace with its reliance on it, and reduced private-sector resilience to cyberattacks on mainland energy infrastructure increases the overall vulnerabilities of UK CNI and CUI.

2.3.2. What can the UK do about it by 2030?

Bolstering the protection of CNI across the UK and of CUI across Europe is a critical component towards insulating the UK from coercive adversary actions and broadly improving societal resilience. However, this will require not only a greater allocation of resources but greater compliance across both government and key private-sector partners, alongside targeted multilateral coordination. Prior RAND research suggests there are a number of actions that can be taken to address the current gaps, including:

- **Effective strategic communication to industry and the public.** Clear directives to key stakeholders will improve the efficiency of decision making at the senior levels and a cross-governmental approach to protecting critical infrastructure both before and during crisis. However, the information-sharing gap between private operators and government will need to be addressed to create an environment of sustained resilience.[20]
- **Expand joint and multilateral detection, deterrence and monitoring operations.** NATO's Baltic Sentry and the UK-led Nordic Warden operations have already produced measurable effects on reducing Baltic Sea drifting activities to reduce cable interference.[21] While continuous monitoring of all CUI remains prohibitively expensive due to the vast geographical area covered, greater multilateral cooperation can enable more efficient use of scarce resources and prioritisation around the most critical areas of concentrated CUI. Nations should invest in regular risk assessment and vulnerability mapping, alongside identifying strategic transit routes and naval choke points that are at heightened risk of adversarial targeting.
- **Ensure greater cybersecurity measures are taken to reduce CNI susceptibility to disruption.** Although more recent cyberattacks on energy infrastructure have failed to cause disruption to the wider energy grid, they are nonetheless indicative of the substantial threat CNI faces from both physical degradation and cyberattack.[22] However, one of the key barriers to developing stronger cybersecurity and resilience measures continues to be a lack of sufficient resources and insufficient compliance to necessary cybersecurity measures.

2.4. Vignette 4: Managing pressures on the health system

February 2030

A coordinated set of cyberattacks targets NHS pathology services across five large hospitals in January, compromising data integrity in their networks – including altering records across a range of categories. The discrepancies are not noticed immediately but once picked up trigger panic within the service. Unsure of what digitised data might be

false, they are forced to revert to keeping manual records with paper and pen, which quickly adds to the confusion. It is months before integrity can be restored, by which point patient backlogs have grown significantly.

May 2030

Upon the outbreak of war, the MOD mobilises the Reserves, including Royal Army Medical Service (RAMS) reservists and Navy and RAF counterparts. Many of these are pulled from the NHS, where they work normal jobs as clinicians. The additional pressure that losing these staff places on health services begins to show almost immediately, with extended delays and cancellations as the NHS scrambles to deal with a reduction in its workforce.

June 2030

When a drone hits a London hospital treating casualties from Estonia, killing 4 people and injuring 15 more, it causes an immediate panic among both patients and NHS staff across the country, who no longer believe themselves safe. Under significant political pressure, the government immediately directs the UK Armed Forces to protect hospitals, stretching the UK's limited air defence and counter-uncrewed air system (C-UAS) capabilities even further and risking significant gaps in the protection of deployed forces and critical military sites.

July-November 2030

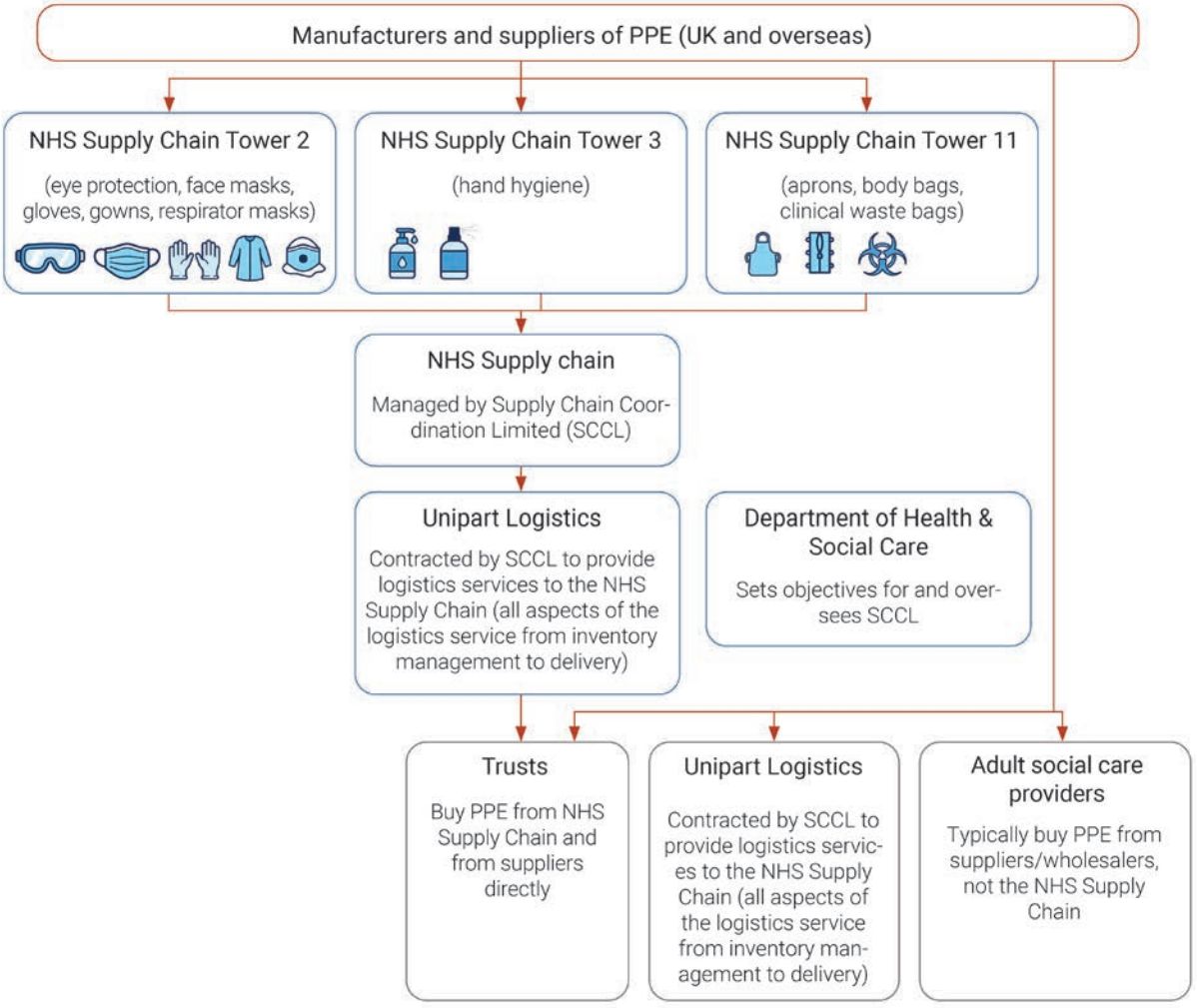
As casualties from the frontline stream back to the UK and mass casualty events from targeted kinetic strikes on the homeland add up, the NHS nears breaking point. Patients are set up on the floor in corridors, standards of care are often not met as staff struggle to attend to everyone, and emergency rooms are overwhelmed. Standards of care continue to decrease as stocks of some pharmaceuticals and medical equipment run low and staff burn out, with the health system facing its darkest period since the worst of the COVID-19 pandemic.

2.4.1. What is the broader problem?

The NHS plans for contingencies and crises, but the reality is that the UK's health service is under acute pressure even in peacetime – let alone a conflict scenario. There are significant vulnerabilities around infrastructure (even down to a lack of beds in hospitals), workforce availability and morale, and equipment like personal protective equipment (PPE). These are feeding a capacity crisis. In a wartime scenario, the NHS is unlikely to be able to scale care further to deal with mass casualty events. Indeed, with many military Reservists' day jobs being NHS roles – leading to them being 'double counted', with HR departments unaware – in the event that the military calls up the Reserves, this would actually apply even greater pressure to an already-struggling domestic system by removing staff at exactly the moment they are needed most.[23]

Supply chains are a crucial concern but often understated compared to more visible issues involving the workforce or physical infrastructure. Not only is supply optimised for peacetime demand (meaning there is little to no surge capacity to draw on), it is also reliant on imports (e.g. for active pharmaceutical ingredients [APIs] availability of raw materials and manufacturing lead times – all of which the UK should expect to be severely disrupted in the event of a conflict. Moreover, it is difficult to map and monitor the supply chain. For example, responsibilities for procurement in the pre-pandemic PPE supply chain were spread across lots of public and private organisations, creating a confusing and overlapping network.[24]

Figure 4: Pre-Pandemic PPE Supply Chain



SOURCE: National Audit Office (2020).

Meanwhile the UK's health system in general is a potential soft target for adversaries. Its digital systems are not sufficiently secure – cybersecurity is a key area of vulnerability, and one that could easily be targeted in a transition-to-conflict phase with long-term implications – and in wartime, the physical infrastructure would be equally vulnerable to threats such as drones, missiles or saboteurs.[25] Contrary to the Geneva Convention, hospitals in Ukraine have been repeatedly targeted by Russia, demonstrating that hospitals can no longer be safely assumed to be 'off-limits', and they lack physical protection.[26] Both in the lead-up to and during a conflict, the NHS will have a key role in the UK's ability to absorb and respond to shocks; it is therefore likely to be a valuable target for adversaries, and one which currently is exposed. In extreme scenarios, there is also the potential threat of the UK's adversaries using bioweapons, forcing a pandemic-style response by both civil and military authorities.

2.4.2. What can the UK do about it by 2030?

Resilience in the health system is crucial to generating resilience in society as a whole. Alongside the need for cross-governmental coherence and coordination discussed above, there are a number of sector-specific priorities that stakeholders in the UK health system should focus on addressing:

- **Invest in network resilience to reduce exposure.** NHS networks, whether digital or physical (e.g. energy infrastructure), are exposed to threats like cyberattacks or sabotage. Investing in more robust cybersecurity, testing and evaluating critical systems, and mapping of and planning for vulnerabilities and dependencies throughout the NHS's supply chain can reduce the threat surface and minimise disruption. Physical hardening or defence against kinetic attacks is a more complicated matter which will involve engagement with the MOD to determine what protective measures can realistically be taken with finite resources.
- **Ensure a joint civil–military medical workforce approach.** A coordinated approach to workforce management could help to deconflict between domestic and military medical services, allowing for more realistic planning. For example, a joint civil–military workforce register could overcome the 'double counting' issue. This approach could also include knowledge transfer via personnel exchanges to develop and maintain knowledge of common military injuries and trauma among civilian staff who may be expected to deal with these kinds of casualties in a conflict scenario.[27]
- **Explore alternative options to surge capacity in a crisis.** The NHS already plans for contingencies, but it is operating at stretched capacity in peacetime. Increasing surge capacity is perhaps the greatest challenge it faces, and there are no easy solutions without unrealistic increases in funding. Dealing with this reality will require innovative national- and regional-level approaches (for example, finding ways to integrate the UK's voluntary/charity organisations like St. John's Ambulance, or even first-aid trained members of the general public, into a response) and also potentially the development of international arrangements among allies and partners to support each other and shore up medical systems across borders.[28]

- **Learn lessons from previous crises.** In particular, the COVID pandemic put enormous pressure on the NHS. Although a very different context from a conflict, the UK can draw several lessons from the response to the pandemic. For example, the setting up of the Parallel Supply Chain (a plan of action to ensure effective distribution of PPE), while successful, was noted by the National Audit Office (NAO) to be a largely reactive effort, with governance arrangements developed over time during the pandemic itself.[29] The core steps of the chain – plan based on expected demand in a crisis, identify surge sources of supply, and create a distributed network for delivery – can and should be set up pre-crisis. Nor would the effort be redundant, as resilient medical supply chains would be hugely beneficial to the NHS in any kind of crisis, not just a potential future war.

2.5. Vignette 5: Contesting the cyberEM domain and AI risks

2028–2029

The UK begins to experience a notable uptick in hybrid activity, particularly a sizeable increase in cyber incidents. Russia deploys AI-enabled malware to disrupt UK military and civilian networks, starting by primarily targeting low-level but frequent attacks on CNI, communication services and day-to-day services through the exploitation of the growing interconnectedness of devices and systems. The malware is polymorphic and adapts to changing circumstances, making the task of defenders increasingly complex and the attacker difficult to decisively attribute. In the UK, it is not fully clear if the attacks being launched are sanctioned by Russia, if the attacks are being made to look like Russia, or if the systems of agentic AI are acting autonomously.

April 2030

As NATO cyber teams prepare contingency plans for the outbreak of war, analysts report the sudden loss of several long-held footholds within Russian military logistics networks, with suggestions that the Russians may be using AI to patch their own systems, leading to NATO pre-positioning in cyberspace being lost. Days later, a notable escalation in the cyber domain occurs when a wave of coordinated attacks on at least four UK data centres within the same 48-hour period triggers cascading, widespread outages that temporarily sever access to cloud-hosted government services, mobile banking applications and NHS patient record systems. Initial investigations find that the malware identified across the different sites does not share identical signatures from one target to the next, instead mutating between intrusions, suggesting an even more mature polymorphic malware may be responsible for the latest wave of attacks. The UK National Cyber Security Centre assesses with moderate confidence that state-backed Advanced Persistent Threat groups orchestrated the initial wave of attacks but cannot determine whether the malware mutations were preprogrammed in advance or generated autonomously by the embedded agentic AI. Full service to essential day-to-day services is not restored for a week, by which point the disruptions have visibly strained public confidence in the resilience of the UK's digital infrastructure systems.

August 2030

As full-scale conflict continues to escalate, a further wave of coordinated cyberattacks bridge the Information Technology (IT) to Operational Technology (OT) air gap in CNI systems that were meant to be insulated from such attacks, triggering the simultaneous failure of industrial control systems at four Grid Supply Points feeding the greater London area's National Grid connectivity and causing power outages for millions. Insufficient human fallback redundancies in the control systems prevent quick restoration of service to the substations, leading not only to widespread blackouts across the city and surrounding area, but cascading impact on essential transport services. In the initial wake of the outages, the capital sees the temporarily halting of major rail services, severe disruption to the London Underground, failure of traffic light and control systems across the city, and major delays to air traffic across London airports. Initial cyber responses are able to make manual overrides that bring critical services back online, but at significantly reduced operating capacity, and much of the city is still left with intermittent access to power as the National Grid struggles to make up for the shortfall in energy capacity. Early assessments of the cyberattack are unable to confidently determine the degree of vulnerability remaining in the substation industrial control systems and whether the attacks have been successfully contained and addressed.

2.5.1. What is the broader problem?

More and more devices are connected to the Internet, including an increasing number of supposedly air-gapped CNI systems, making them vulnerable to a wide range of cyberattacks on both IT and OT systems that can cause physical degradation of CNI assets. Because of this interconnection, isolating and containing threats has become more difficult, and containment measures can trigger cascade effects on access to a range of services should key connectivity chokepoints need to be temporarily shut down. Ambiguity in attribution also poses growing challenges to incident response, as evolving AI-related cyber capabilities make it increasingly difficult to distinguish between malicious attacks by human actors, system malfunctions or autonomous AI actions. Further, while AI-connectivity across the UK has increased dramatically, legal and decision-making frameworks have failed to match pace, meaning it is not certain whether clear mandates for ordering emergency shutdowns of AI-connected infrastructure are both sufficient and viable in the event of a crisis. Such connectivity concerns are further exacerbated by the potential erosion of sufficient human fallback and manual override capacity.

2.5.2. What can the UK do about it by 2030?

The mounting threats across the cyber and electromagnetic domain have been clearly recognised across UK and Allied governments, with increasing national, NATO and EU-wide efforts to strengthen cyber defence and security, as well as improve multilateral coordination and cooperation across the cyber threat landscape. However, greater cyber resilience measures are still required, particularly in light of the pace and scope of expansion in global digital connectivity and AI-enabled offensive cyber capabilities. To address these concerns, RAND research suggests the following measures:

- **Build relationships with frontier AI labs to increase understanding of the technology and maintain access to the latest models.** RAND's

ongoing work across the *Infinite Potential* platform has consistently found that developing relationships with cutting edge technology labs will require long lead times, and that rapid access to advanced closed-weight models (typically from the United States) in the event of a crisis may not be possible absent measures taken in advance.[30] Gaps in governance, regulation, and oversight of advanced AI can undermine the UK's ability to shape outcomes and protect its interests as the technology continues to rapidly evolve.

- **Harden cyber defences in critical national infrastructure and maintain human fallback contingencies where possible.** Improving cyber resilience across the UK will require not only sufficient manual override capabilities so that critical sectors can revert to human control when needed but further that there is continued investment in exercising reversionary modes and training key employees to prevent skills erosion in critical sectors.
- **Develop predefined and pre-agreed parallel-response actions to reduce decision-making time delays in the event of crisis.** Building the ability to act rapidly along multiple tracks simultaneously absent clear attribution or full incident reports will better position government and key private-sector industry partners to identify and contain threats as they occur as well as to accelerate the restoration of services should they be disrupted.
- **Cyber threat intelligence teams and frontier AI model labs should develop a widely accessible database of correlations between AI misuse and malicious cyber activity.** A standing database would address both information-sharing gaps currently present between government and frontier AI labs to incorporate privileged information on AI models and sufficiently contextualise the threats in a broader security context as well as to enable faster identification of model behaviours correlating with malicious activity, improving both detection speed and attribution confidence.

2.6. Vignette 6: Contesting the space domain

March 2028

An anonymous actor, which the intelligence community assesses with moderate confidence to be a state-backed Russian proxy, breaks into and takes over the command and control of a UK-licensed commercial satellite. Before control can be restored, several commands are issued which use up the onboard propellant and degrade the lifespan of the satellite. Immediate impact is limited and it remains unclear what the objectives of the attack were – especially whether there was any direct strategic intent.

February 2030

The position of a Russian satellite is adjusted to tail one of the UK military's Oberon Synthetic Aperture Radar satellites along its orbital path. The motive remains unclear until the satellite conducts a rendezvous and proximity manoeuvre (RPO) and closes in on the Oberon satellite. Communications between the Oberon satellite and the ground station begin dropping out. It is assumed that the Russian satellite is electronically interfering with communications. It takes three weeks for communications to be restored to full working order.

May 2030

In the early hours of the morning, thousands of satellite modems go offline across the Baltic States, limiting effective communications between government departments, military units and international partners. Three hours later, Russian troops begin to move over the Estonian border. As NATO reinforcements move into Estonia and full-scale warfighting breaks out, Russia begins deploying offensive counterspace capabilities in support of its forces on the ground. NATO guidance systems struggle on the front as Russian forces deploy electronic warfare (EW) capabilities to jam user terminals at the tactical level, interfering with NATO's deployment of uncrewed systems and guided munitions. Meanwhile, a directed-energy system, assessed to be a *Peresvet* laser, dazzles the electro-optical sensors of Allied satellites as they pass over the front, damaging NATO forces' situational awareness.

September 2030

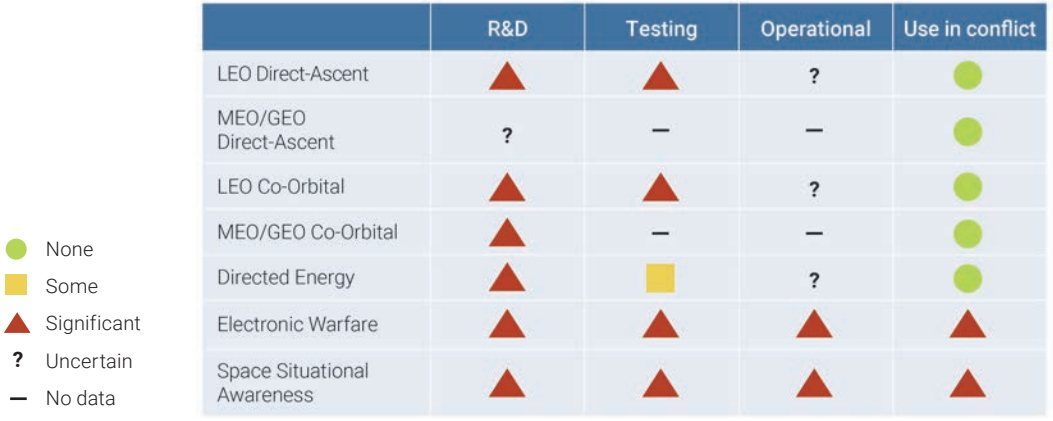
A Russian Cosmos satellite manoeuvres into position around the UK's Tyche satellite, the UK's low-earth orbit intelligence, surveillance and reconnaissance satellite, which has been providing optical data to support NATO operations in the Baltic States. A rapid rendezvous brings the Russian satellite close enough to launch a projectile at Tyche before it can be manoeuvred away. Tyche is not destroyed, but its sensors are heavily damaged, and its operational utility is compromised.

2.6.1. What is the broader problem?

The UK and Europe suffer an asymmetric vulnerability in the space domain compared to Russia. The UK and NATO rely far more heavily on space assets and services to conduct multi-domain operations compared to Russia. Space is a critical enabler, but it is also a critical dependency: the effective operation of Allied forces relies heavily upon the space domain. Nearly every UK capability – command and control, precision strike, intelligence, surveillance and reconnaissance and so on – is dependent on space in some way.

In this context – and as proven by the coordinated cyberattack on Viasat satellite systems that immediately preceded the Russian full-scale invasion of Ukraine in February 2022 – the early hours of a conflict are likely to take place in space, with potentially severe implications for the course of a future war.[31] Russia has developed a robust counterspace doctrine and has been pouring significant R&D effort into the development of a range of counterspace capabilities, many of which appear to be moving towards operational status.[32] Ultimately, the UK is not currently in a position to compete militarily in the space domain without drawing significantly on US capabilities and enablers – running the risk of losing the fight there in the early stages of a conflict (or even before a conflict begins). The UK needs to learn not only how to better protect assets and equities in the space domain but potentially (relearn) how to fight without it.

Figure 5: Russian counterspace capabilities, R&D and deployment



SOURCE: Secure World Foundation (2026).

2.6.2. What can the UK do about it by 2030?

The threat in the space domain is clearly recognised – in September 2026, the UK formed the RAF No.3 Space Effects Squadron sitting under UK Space Command. The squadron's stated operational purpose is to disrupt, degrade and deny hostile activity to protect the UK's interests in space. Its creation is certainly a step in the right direction, but the UK's space capability to counter aggressive and intimidatory space activity remains limited (especially for protect-and-defend missions), and there is a prominent continued mismatch between the stated ambitions of the recent UK Space Strategy and the resources available to realise them.[33]

To address this gap, RAND research suggests that the UK could consider the following[34]:

- **Develop a domain-specific own-collaborate-access (OCA) framework.** Urgent acquisition of capability in certain areas – specifically, capability to better secure and protect the UK's existing assets in space, and capability to address critical dependencies across Defence (e.g. overreliance on satellite communications) – may be more suitable for the UK than entirely UK-based sovereign development. This could involve military-off-the shelf (MOTS) purchases where appropriate ('access'), such as acquisition of the American ground-based mobile jamming counterspace system Meadowlands, which has recently been approved for exports to Five Eyes partners, or targeted niche R&D and manufacturing contributions to international programmes ('collaborate').[35]

Figure 6: The Own-Collaborate-Access (OCA) Framework



SOURCE: Retter et al. (2022).

- **Integrate into international programmes and supply chains for space capability development.** Specifically, the UK should take advantage of its R&D-intensive space industry to foster cooperation. International collaboration will be an important element in acquisition of advance space capability. The UK may be able to develop niche capabilities itself, but its strengths lie in its networks of key alliances and partnerships.
- **Develop alternatives to space, not just in the military domain but across the board.** The UK should invest in redundancies and reversionary modes for critical military and government C2, communications, GPS and positioning, navigation and timing (PNT) systems to ensure that its forces can fight effectively without the space domain if so required.

2.7. Vignette 7: Mobilising people

January 2028 – April 2030

Across UK Defence, the armed forces, government organisations and industry continue to report recruitment and retention issues. In particular, industry reports gaps in critical but niche skills, including welding and aerospace engineers. Despite efforts at incentivisation, including healthy remuneration packages, firms including BAE Systems consistently report shrinking workforces in their

annual reports. While some of this is attributed to ongoing malicious activity targeting Defence personnel (including online threats against individual and family safety and attempts at blackmail), it is acknowledged that this is part of a broader trend that government and industry together have failed to address over many years.

Especially in the context of active fighting ending in Ukraine, the view that defence should be deprioritised slowly gains traction, fed by media and online narratives that Russia is no longer a military threat. An April 2029 poll conducted by a reputable independent organisation suggests that the UK population – and the overwhelming majority of young people – believe that defence spending is excessive and that resources should be reassigned to struggling domestic services like the NHS. Crucially, despite efforts to increase the appeal of Defence careers, the majority of young people would not consider a career in Defence – largely driven, it seems, by ethical concerns and the belief that the primary threat to the UK (Russian hostility) ended with the war in Ukraine.

May–November 2030

On the outbreak of war, the British Army's 3rd Division is deployed to the Baltics to support the eFP presence, with the armoured brigade contributing to NATO efforts on the ground. However, on top of the weeks taken to bring the 3rd Division to full operating strength, by the start of July, heavy casualties in UK-led formations minimise their operational value. The Regular Reserve is quickly mobilised to fill the gaps but fails to perform to the same operational standard. By August, the UK's deployed fighting strength on land is exhausted, with no options to replace it without a political decision to implement conscription.

Meanwhile, the Royal Navy mobilises the surface fleet and all available submarines to meet directives to protect the North Atlantic SLOCs, conduct ASW operations, and generate a carrier strike group to threaten Russian forces and locations around the Atlantic and High North as necessary. However, in the context of ongoing, years-long crewing shortages, the Royal Navy is forced to choose between tasks, while some frigates are left short-handed and unable to be deployed for ASW duties.

Despite efforts in recent years to re-focus on control of the air, the RAF's diminished fighter fleet is unprepared for a battle of attrition in the skies or for suppression of enemy air defences, with damage to aircraft soon matched by casualties among F-35B and Typhoon pilots. Even before UK industry exhausts its spare parts pool for the platforms, air sortie rates are impacted by a diminishing pool of pilots. With a longstanding training backlog, replacements cannot be deployed immediately. By August, the high rate of attrition has exhausted RAF depth not just in pilots but in ground crew too, effectively grounding the combat air fleet for all but the most critical of operations.

2.7.1. What is the broader problem?

Recruitment and retention approaches have not been updated to reflect the skills required for an effective contemporary Defence workforce. In particular, practices have failed to effectively reach communities beyond the 'traditional' recruitment pools.[36] As a result, as of April 2026, none of the three UK armed forces services have met their target sizes in terms of trained strength, and gaps in critical skills persist across defence industrial sectors.

Figure 7: UK armed forces performance against trained strength targets

Performance against armed forces strength targets by service branch
Full time trained/trade-trained strength against target: 1 April 2026

	Army	RN/RM	RAF	**Total**
Current target	73,000	30,450	31,750	**135,200**
Trained strength	70,759	28,182	27,800	**126,741**
Surplus/Deficit	-2,241	-2,268	-3,950	**-8,459**
% above/below target	-3%	-7%	-12%	**-6%**

Note: targets are based on the trained strength of the RN/RM and RAF and the trade-trained strength of the Army

SOURCE: Ministry of Defence, Quarterly service personnel statistics: 1 April 2026

In terms of the armed forces, although there is a growing discussion of the need for more Reservists – and to increase their involvement in Defence – this is largely impractical as it stands. Surprisingly little is actually known about the Reservists already in service and the challenges they face, and as a result, it is difficult to develop suitable policy to improve recruitment and retention. At the same time, scandals across the sector continue to highlight significant cultural challenges in the Defence workforce and among Defence leadership, which hinders progress.

The defence industry faces similar problems in terms of recruitment and retention, but they manifest in different ways. While there is certainly a 'mass' issue as there is with the Services, in industry, the most prominent shortages manifest in highly skilled, critical, but often niche skills.[37] Specialist welding is an example from the maritime surface and subsurface industries which requires years of experience to master but is a relatively unknown career path.

These highly specialised skills act as effective bottlenecks in industry in the same way as a valuable component – without it, programmes simply halt. Recruitment in these fields is becoming more difficult, especially in non-digitised manufacturing roles, but retention is also a massive issue – in sectors such as combat air and naval shipbuilding, commercial companies working on adjacent civilian programmes can offer lucrative remuneration and benefits packages that are difficult for Defence to compete with.[38]

More broadly, there is a lack of connectivity between the civilian population and Defence. This manifests in a misunderstanding of what Defence is for, what opportunities it can provide – and thus perceptions of Defence that does not lend itself towards effective recruitment and

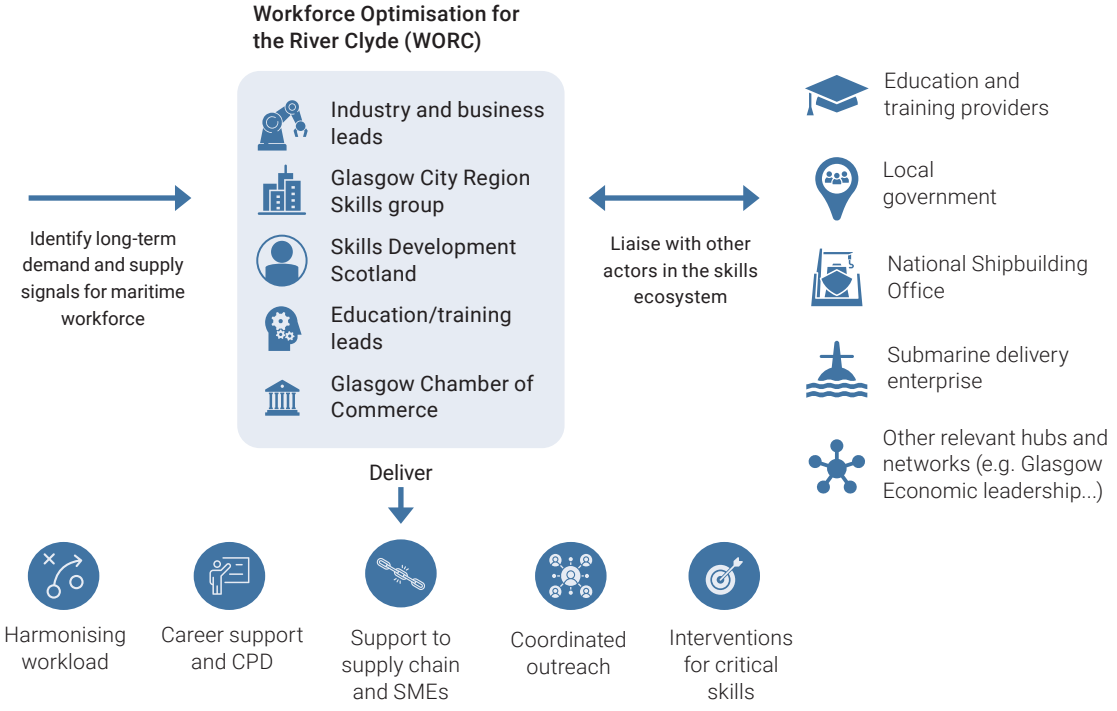
retention.[39] This is, at its heart, a communication issue between government, Defence and the wider population.

2.7.2. What can the UK do about it by 2030?

Changing attitudes towards Defence as a career is a long-term process that will certainly not be fully complete by 2030. However, there are some steps that the UK can take to at least begin to change some overarching workforce trends:

- **Streamline and target recruitment processes for specific skillsets.** By strategically targeting recruitment materials for specific roles and skillsets while also making the application process easier, the right people can be brought into Defence. Recruiters need to make clearer the skills that are desirable for various Defence roles, and perhaps more importantly – the range of opportunities that exists within the sector. The Defence Technical Excellence Colleges, which provide training in crucial defence industry skills, provide a good base to build from in terms of providing tangible opportunities with concrete career pathways for younger generations.
- **Increase engagement with other sectors and the public.** This should include sectors like education, which can enable engagement with the younger generations, but also sectors like healthcare that have more niche applicability (e.g. NHS staff could become medical corps reservists). Defence should be promoting awareness of opportunities cross-sector and across the board – especially in the context of the increasing importance of societal resilience, the core message needs to be that everyone has a role to play in the UK's safety and security.
- **Develop incentives that reflect modern ways of working.** There are plenty of roles in Defence that do not require 'traditional' military skills but instead reflect the increasing digitisation of Defence and its workforce. This of course also reflects broader trends in society towards digitisation, which comes with changing expectations of the workplace: Defence must consider where it can adapt its more traditional approaches and expectations to increase its appeal.[40]
- **Encourage an enterprise approach to industry workforce planning.** As it stands, there is often competition for skills from a limited recruitment pool both between firms in the defence industry and between defence and civilian sectors. By creating formal opportunities for collaboration on workforce issues – for example, the Workforce Optimisation for the River Clyde group concept recently proposed by RAND Europe for the naval shipbuilding industry – coordinated, enterprise-level planning can be established across industry, government and even sectors like education, creating a coherent network to support the development of a healthier workforce.[41]

Figure 8: Proposed functions for a coordinated naval shipbuilding workforce optimisation group



SOURCE: Retter et al. (2025). While specific to the naval shipbuilding sector, this illustrates the range of benefits that an enterprise approach to workforce planning could achieve.

2.8. Vignette 8: Mobilising industry

2028–2029

In the early months of 2028, defence industry companies report a growing number of security incidents targeting their staff at all levels of seniority, including directed communications over professional networking platforms, social media and WhatsApp. Although approaches initially seem relatively harmless, incidents begin escalating into attempts at blackmail and threats against the safety of individuals and their families. The 2029 annual reporting of major defence industry players, including BAE Systems,

indicate a concerning struggle in retention, while recruitment numbers go down. Privately, the problem is attributed to some workers no longer perceiving the defence industry as a safe and secure working environment.

Concurrently, pre-existing strains on global supply chains are exacerbated and single points of failure are exposed when Tier 3 suppliers, both domestic and those based overseas, are disrupted by a seemingly random wave of cyberattacks, including intellectual property (IP) theft, ransomware and service compromise. Several incidents are traced back to suspected Kremlin proxies, but nothing can be definitively attributed to a hostile state. Under pressure from consistently delayed shipments of critical components and a reduced effective workforce in industry, the UK MOD is forced to revise timelines for the delivery of strategic capability programmes.

January–April 2030

Disruption across key defence industry sites intensifies. Primes report attempts to overcome physical security at key sites including the submarine yard in Barrow-in-Furness, naval facilities at the Clyde, the missile manufacturing site in Bolton, and munitions factories at Radway Green and Glascoed. In a few instances, the perpetrators are successful in gaining access to the sites. The most serious incident is a case of arson at the Venturer assembly hall in Rosyth. Emergency services are able to save the building, but the facilities inside are gutted. Internally, Babcock estimates that the Type 31 programme will effectively be on pause for at least six months while repairs are made.

In April, an anonymous hacker group uses a spear-phishing attack to instal malware on an industry server used to host classified working, encrypting access and releasing both sensitive information relating to defence programmes and personal data about senior executives at the company. A major firm shuts down its systems in response, reverting to in-person and handwritten communication for all sensitive work until control can be restored and the extent of access and damage to its systems can be properly assessed. Both internal communications and communication with industry partners and the MOD becomes sluggish, and progress across core capability programmes grinds to a halt.

May–November 2030

At the outbreak of war, industry is called upon by the government to scale up production and ensure it can sustain capability through the conflict. The primes, headed by BAE Systems, attempt to organise a coherent response, but in the context of years of supply chain disruptions and damage to key industrial sites, they face challenges to support repairs to the UK's damaged surface combatant and aircraft fleets, let alone meet complex weapon and conventional munition demand. Platforms damaged in the early stages of the war are consigned to sit by as industry struggles to source enough spare parts to repair them and get them back in the fight.

As the war drags on, targeted Russian strikes and a coordinated sabotage campaign on the UK homeland begin to include key defence industrial infrastructure in an effort to disrupt production. Barrow-in-Furness, shipyards along the Clyde, and smaller defence industrial facilities across the country including Swindon, Glascoed, Bristol and Derby all sustain damage as strikes saturate the limited air defence capability. Production capacity is hit hard, with no latent capacity in the UK system providing any flexibility to adapt after core sites shut down.



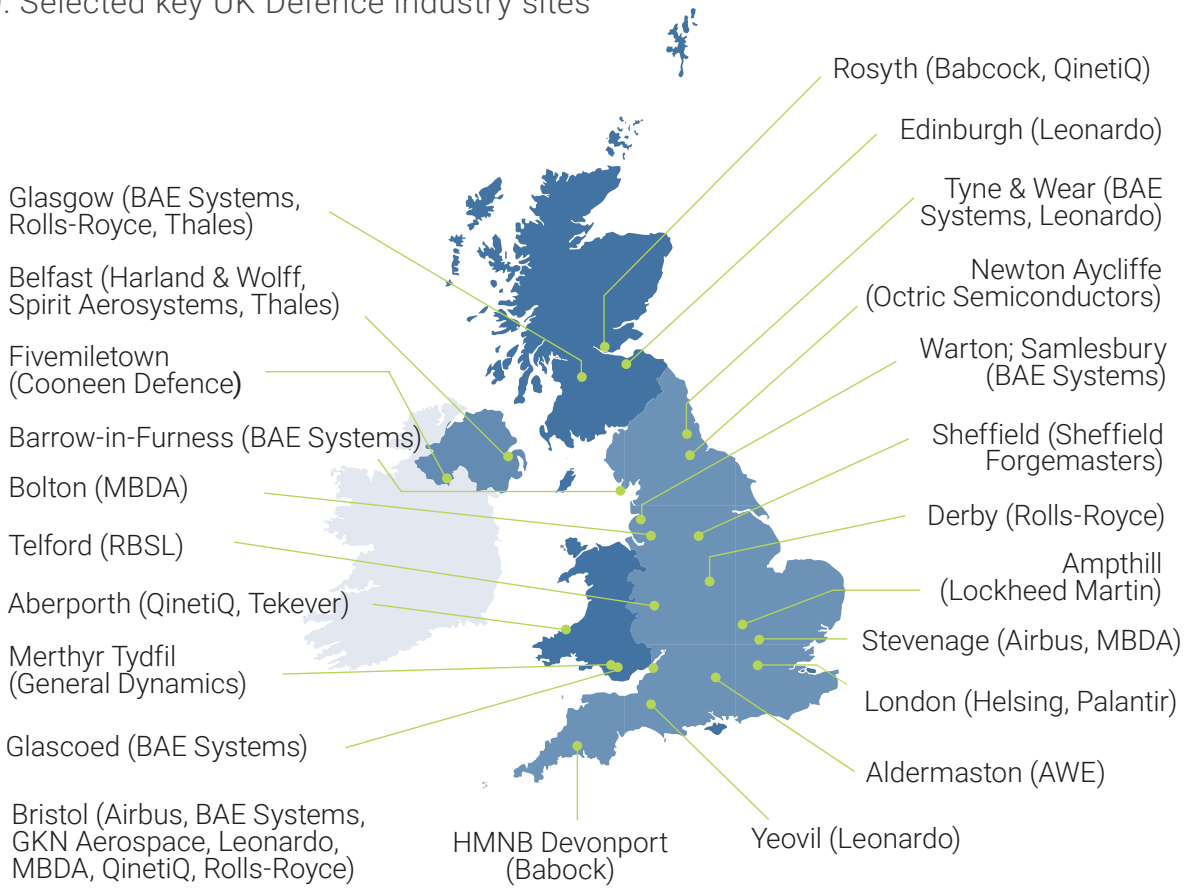
UK MOD © Crown copyright 2024

2.8.1. What is the broader problem?

The core issue facing the UK's defence industrial base is significantly limited capacity. The UK's stockpiles – particularly those of complex weapons and conventional munitions – have been depleted supporting Ukraine, and to date, efforts at scaling production have been barely sufficient to restock them, let alone build them up to wartime levels. Moreover, the UK's emergency powers regime to transition into crisis mobilisation of industry is rooted in an outdated interpretation of 'emergency' that includes a clearly defined crisis point.[42] This point may come late, as demonstrated in this vignette – or perhaps even not at all. The vignette demonstrates in extreme terms how vulnerable the UK's defence industrial base currently is to erosion of capacity through a long-term accumulation of subthreshold actions, none of which are sufficient to trigger emergency/crisis scale-up under current policy.

The UK's defence industrial base is ultimately an extension of the wider conversation around the importance of resilience across the spectrum of conflict. Kinetic strikes on single points of failure in the UK defence industrial ecosystem (see Figure 9) are a possible but extreme problem – the more concerning vulnerabilities may in fact be the critical gaps that deprive the defence industry of the necessary resources (across materials, workforce and systems) to produce and sustain in the long term, which may be sufficient to undermine its utility in a crisis before the first shot is fired.

Figure 9: Selected key UK Defence industry sites



SOURCE: Ministry of Defence (2025).

2.8.2. What can be done about it by 2030?

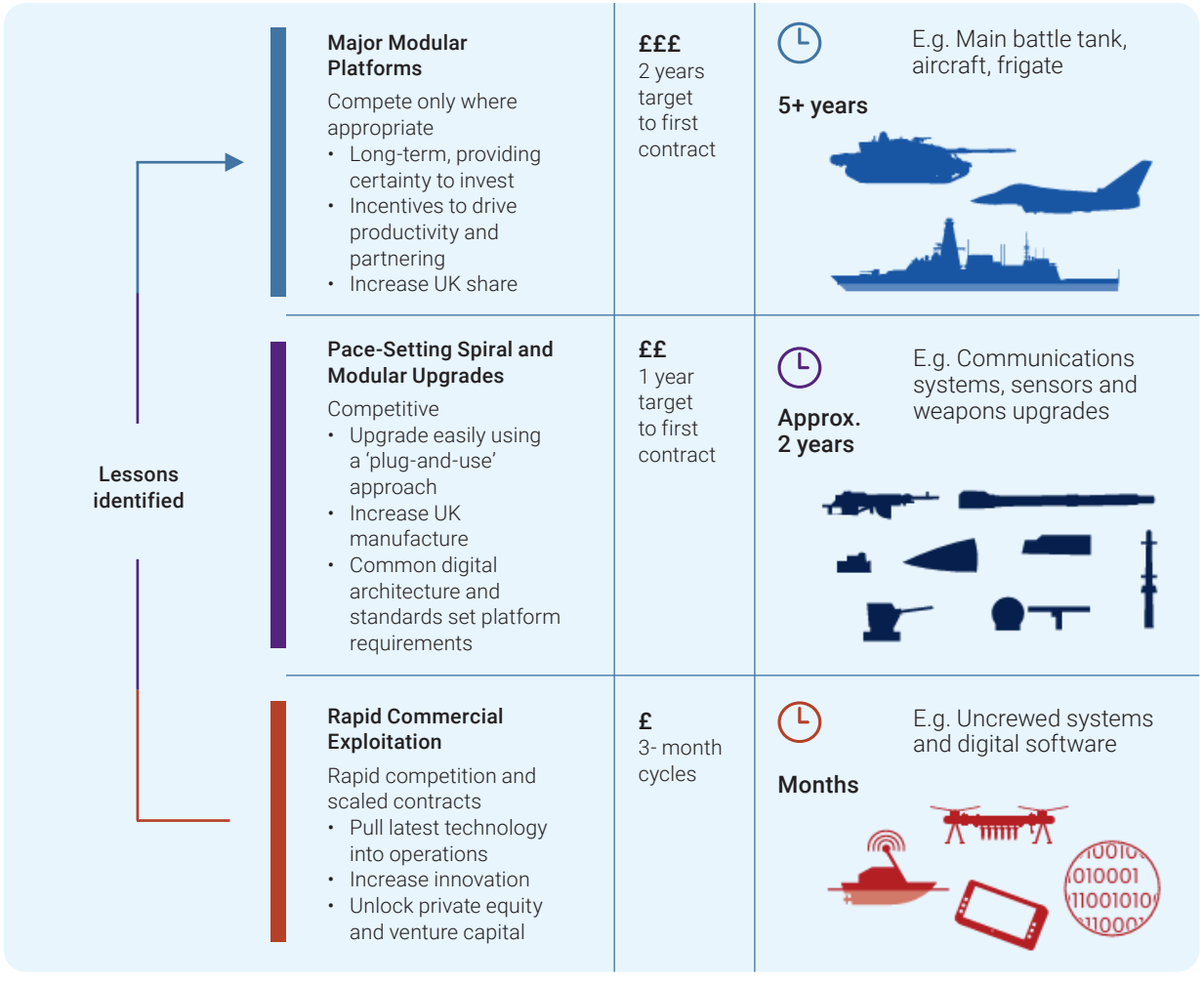
The UK's defence industrial base is brittle and vulnerable across the board as it stands, from exposure of both physical sites and digital networks to hostile actors, to supply chain and legal issues that generate broader weaknesses across the ecosystem. None of these issues can be addressed quickly in full, but there are several steps the UK can take to work towards resilience and preparedness in its defence industrial base:

- **Physical hardening of key sites.** Currently, many defence industrial sites present soft physical targets, with no consistent application of security

measures. Creating resilience will involve introducing redundancies (e.g. for power supplies), security measures not just at the sites themselves but at the nearby transport links/hubs providing access for workforce and supplies, and potentially geographic dispersal – where possible – to reduce the number of single points of failure and minimise the impact of an event damaging production capacity (whether pre-crisis, such as sabotage/arson, or intra-war through kinetic strikes) at any one site.

- **Raise cybersecurity standards throughout the supply chain, including subthreshold threat awareness.** This could include simple steps to prevent cyberattacks, including multi-factor authentication and access management, which are generally practised by primes and Tier 2 suppliers, but the extent of coverage is uncertain at Tier 3 and below. Meanwhile, if an incident does occur, prearranged response plans – including offline reversionary modes and segmentation of sensitive data – can help to mitigate the impact. Primes should play a key role in coordinating and delivering cyber security across the supply chain – the defence industrial base is already consolidated around them, so they are naturally suited to a taking leading role on this front.
- **Stockpile long-lead components.** Especially regarding bespoke components for exquisite capability (for example, spare parts for combat aircraft or surface combatants), these generally cannot be acquired quickly and delays are likely even for urgent orders (indeed, the Global Support Solution for the F-35 programme was determined insufficient to support the UK's stealth fighters by the NAO in 2025, even outside of a crisis scenario).[43] By stockpiling these components, the UK defence industrial base can increase its capacity to absorb shocks in a crisis and continue sustainment of the UK's defence capability.
- **Determine appropriate increases to risk appetite and modernise procurement pathways to prepare for a crisis.** Outside of the declaration of emergency powers, there is currently little to no flexibility in terms of speeding up lengthy processes like fulfilling procurement regulations and assurances, Test & Evaluation and contracting. Initiatives like Commercial X, an MOD team empowered to streamline procurement processes in certain sectors, and the new segmented approach to procurement announced in the Defence Industrial Strategy, provide a starting point and should be expanded upon (see Figure 10).[44] Designing pre-agreed expedited pathways for rapid urgent procurement for activation on 'day one' of (or more accurately, the 'day before') a crisis is a choice that will have long-term consequences (e.g. potentially limiting the UK's future export base) but may well be necessary to fight and win a future war – particularly if a traditional 'crisis point' triggering emergency powers is never reached.[45]

Figure 10: The MOD's Segmented Procurement Strategy



SOURCE: Ministry of Defence (2025).

- **Map and secure the supply chain.** A focus should be placed on identifying and mitigating single points of failure in the broad and disorganised network of Tier 3+ suppliers.[46] Approaches to mitigation could involve acquisition, bringing critical dependencies within the purview of a trusted prime, or in the case of overseas suppliers, encouraging onshoring or friend-shoring to ensure secure localised supply chains that are more reliable in a crisis than globalised counterparts.

2.9. Vignette 9: Managing threats to air and missile defence

2028–2029

Sporadic incidents involving unarmed uncrewed aerial systems (UAS) around airports, energy infrastructure and other CNI increase in frequency around the UK. Most of these involve short-range drones launched from nearby, but two incidents involve unattributed UAS launched from offshore. The providence is unclear. UK authorities respond reactively and ad hoc, with no coordinated organisation of resources at either the local or national levels.

January–April 2030

UAS activity begins to concentrate around key defence sites, including the RAF bases at Brize Norton, Fylingdales and Lossiemouth. Each incident forces a response and disrupts activity in the airspace around the military installation. In February, one incident involves the use of improvised kinetics on a small UAS. Authorities detain the perpetrator but are unable to determine whether they acted alone or under instruction. From this point, the armed forces are instructed to shoot down UAS around critical sites. However, this strains the UK's already-limited stocks of interceptors and numbers of trained counter-UAS (C-UAS) specialist teams. Pressures and gaps in C-UAS capability across the UK begin to show just as the frequency and intensity of incidents begins to step up.

May–November 2030

As part of the Russian campaign to limit NATO's strategic flexibility and pose dilemmas to the Alliance, a wave of targeted long-range precision strikes hits key military locations around the UK. Submarine- and aircraft-launched missiles, along with UAS launched by covert Spetsnaz teams operating from civilian ships, vehicles or remote locations in the UK and Ireland, mean that the UK finds itself threatened from multiple vectors. This creates dilemmas about where to focus the UK's finite air defence capabilities.

Russia attempts saturation attacks in an effort to exhaust kinetic interceptor stocks and stretch combat aircraft used for response, before coordinated strikes using conventionally-armed cruise and ballistic missiles and a small number of hypersonic weapons are launched across bases at Portsmouth, Faslane, Coningsby and Lossiemouth. Two Type 45 destroyers on station intercept some strikes, but Aster missile stocks begin to run low even after the first wave.

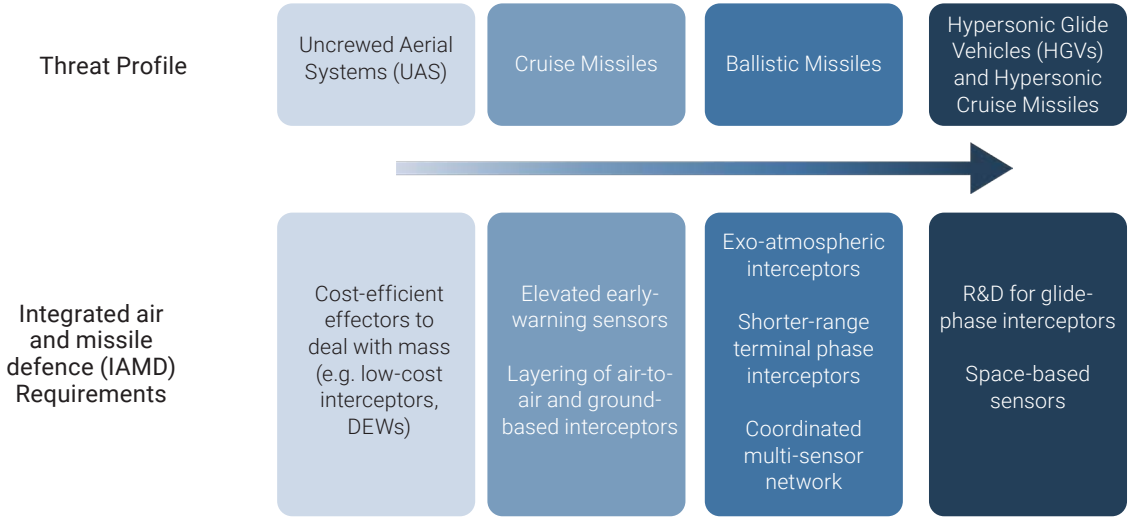
The second wave of strikes targets defence industrial nodes, designed to nullify any potential scale-up of UK capability production. By this point, the UK's already-limited air defence capability has been severely stretched and cannot defend many targets. Military-to-military communications confirm that the next wave of strikes intends to

escalate further and use hypersonic and ballistic missile assets to target civilian infrastructure nodes – including the National Grid control centre, gas import hubs, and major ports and airports.

2.9.1. What is the broader problem?

Air defence constitutes an expanding domain with an increasingly blurred set of remits. Emerging technologies – most prominently, UAS – are transforming the threat environment, which is now both diverse and saturated. Threats range from small UAS to sophisticated combat aircraft and a wide variety of cruise, ballistic and hypersonic missiles launched from land, air or sea – there is an entire spectrum of aerial threats, each of which requires different tools to defeat.

Figure 11: Likely aerial threat spectrum by 2030



SOURCE: Adapted from Kaushal (2025).

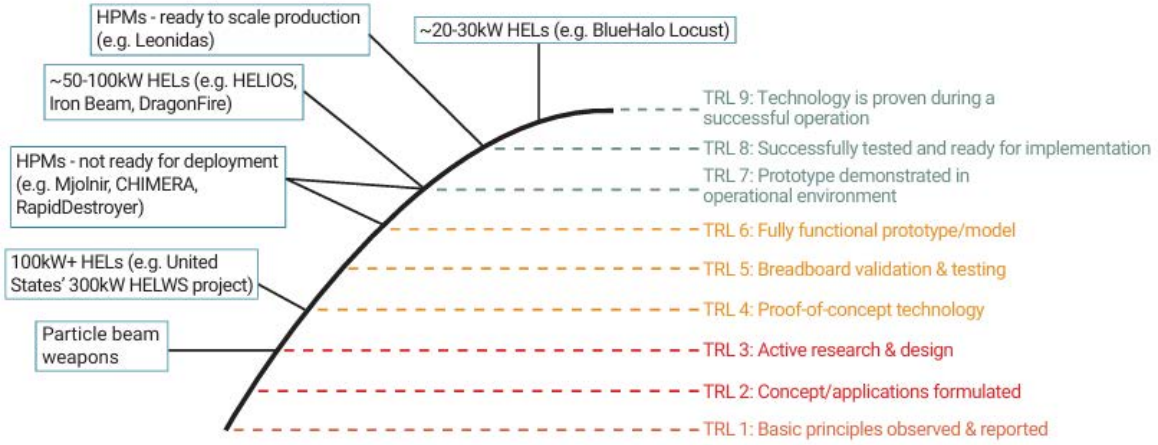
In contrast, the UK's response options are currently fragmented and poorly orchestrated, built around an out-of-date conception of air defence that is focused on high-end missile threats. Until recently, this has arguably been sufficient, with no other threats realistically focused on targeting the UK homeland – particularly in the context of limited wars of choice, far from the homeland and fought against non-peer adversaries.[47] The contemporary threat environment has now evolved far beyond this, for example through long-range or locally launched armed UAS – the UK's only option as it stands is the use of expensive interceptors such as the Aster to target comparatively cheap one-way systems, which is completely unsustainable. Without a multi-layered, integrated air and missile defence (IAMD) network that has tailored options to respond to different kinds of threats, the UK will remain vulnerable. Though the UK MOD has recently established an IAMD Directorate and pledged to invest in growing IAMD capability through the Defence Investment Plan, spending remains low relative to the scale of the challenge.

2.9.2. What can the UK do about it by 2030?

The UK is already exploring options for future air defence, ranging from cheap interceptors to directed-energy weapons (DEW). There are plenty of potential solutions that could be integrated into a multi-layer integrated air defence system (IADS), but investment into development and acquisition will need to be carefully sequenced and prioritised given the cost. Steps towards this should include:

- **Explore and invest in options to acquire cheap interceptors.** There is an emergent market of start-ups and SMEs in the UK – including companies such as Cambridge Aerospace, Frankenburg Technologies and Tiberius Aerospace – which are developing both the systems and novel industrial set-up concepts to help scale production to the level required. Simply put, in a saturated threat environment, cheap mass to counter the sheer number of likely threats will be incredibly valuable. These capabilities could help the UK achieve a balanced ('high-low') air defence capability suitable for dealing with the diversification of threat profiles in this domain, while retaining its limited stock of expensive interceptors for exquisite threats.
- **Fund R&D for novel emerging technologies that hold promise to enhance air defence capability.** Effective development and exploitation of emerging and disruptive technologies (EDTs) will certainly be a long-term component of the solution. Directed-energy weapons (DEWs), for example, have been the subject of scrutiny in recent years and appear to be shifting from R&D towards operational deployment.[48] DEWs provide low cost-per-shot effects that can certainly contribute to C-UAS, but there are several technological limitations (e.g. beam scattering) and enabling factors (e.g. suitable energy sources) to overcome before this can be realised.[49] They are a long-term aspiration based on current Technology Readiness Levels (TRLs – see Figure 12). Regardless, DEWs certainly do not represent a panacea for air defence and should make up just one element of the future IAMD toolkit rather than being the focus.

Figure 12: Illustrative DEW TRLs



SOURCE: Dee et al. (2025). Note: HEL = high-energy laser, HPM = high-powered microwave system.

- **Engagement with international partners on collaborative air defence capability acquisition**. This could provide pathways to rapidly shore up existing gaps in this domain. The UK is already a participant in the German-led European Sky Shield Initiative (ESSI), which aims to streamline acquisition of proven MOTS capability – addressing urgent operational requirements, generating economies of scale and ensuring continued Alliance interoperability at the NATO level.[50] However, the UK should be selective in which programmes it engages with – ESSI, for example, has come under criticism for its significant reliance on the United States or Israel for the technology and some systems (in particular, the long-range layer, for which the US Patriot remains the main system of interest, and the exo-atmospheric layer for ballistic missiles, for which it proposes use of Israeli Arrow interceptors).[51]

2.10. Vignette 10: Managing threats to critical military capabilities

January–April 2030

In response to increased (suspected) Russian disruption and military manoeuvring in Russia's Western Military District, the NATO Allied Rapid Response Corps (ARRC), headquartered at Imjin Barracks in the UK, deploys a forward command node to Tallinn, as much for operational planning as for strategic signalling. Meanwhile, ARRC staff in the

UK are recalled from leave and the British Army's 3rd Division is moved to a state of high readiness. Planning for transit to Marchwood and embarkment there begins.

May 2030

Upon the outbreak of war, the ARRC is assigned as a corps headquarters to be deployed in Estonia under JFC Brunssum, commanding the UK's 3rd Division alongside two Allied divisions. However, with competing claims across the Services for strategic sea- and airlift, transfer into theatre is disjointed and confused. Even once the ARRC reaches Estonia, it takes days to orchestrate corps-level capability (e.g. logistics, ISR, deep fires) at its command. Meanwhile, unexpected delays in the 3rd Division preparing for deployment mean they do not reach Marchwood until mid-May. By this time, long-range Russian strikes, saboteurs and cyber-attacks have begun targeting strategic hubs including ports and airbases, causing further delays as infrastructure and transport platforms are damaged. The ARRC is uncertain when exactly it can expect the division's brigades to be available for tasking. By the time the ARRC is ready for action, Russian armed forces are dug in around Narva beneath a dense IAMD network with heavy EW coverage, restricting the potential for any rapid NATO counteroffensive.

June 2030

An Astute-class nuclear-powered submarine (SSN) is sunk during the ASW campaign in the North Atlantic and High North. A week later, another suffers damage from a Russian torpedo and limps back to Devonport, where it remains for months as it awaits repair. With two boats undergoing long dry-dock maintenance periods that had begun before the outbreak of war, the UK is left with just two SSNs on hand – for which regular maintenance has been deferred – less than six weeks into the war. When a technical failure puts one of these boats out of action in mid-July, the UK has to make do with just one SSN holding Russian assets in the Atlantic and High North at risk.

2.10.1. What's the broader problem?

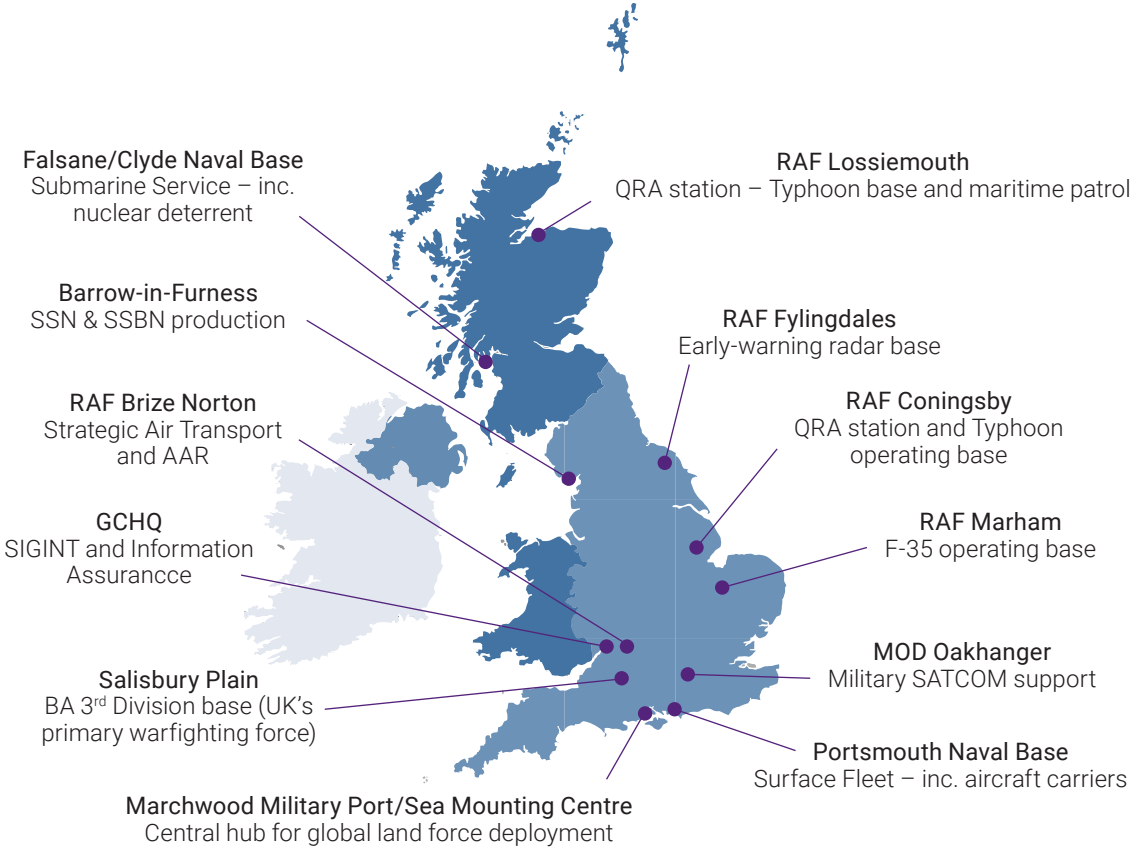
The reality of the UK's force offer to NATO is that frontline mass is neither its strength nor its priority. The UK defence ecosystem is built around the concept of technological integration and precision over mass, and in this context, it provides the Alliance with a set of strategic capabilities that very few European Allies can – specifically, advanced C4ISTAR, air-to-air-refuelling, SSNs and, most critically, the continuous at sea deterrent (CASD). It also provides strategic depth and a logistical hub linking the North Atlantic theatre and SLOCs to Europe, as well as having NATO's AARC headquartered in Gloucestershire.

However, this portfolio of capability is built largely around exquisite capability with limited depth – indeed, some of the UK's flagship capabilities (e.g. its Astute-class SSNs) do not exceed single digits in terms of units. Simply put, the UK's core strategic capabilities might be technologically superior, but they lack mass, are brittle, and are at risk of failing operationally in the face of high attrition rates. The UK's military capability has over the course of decades been optimised for limited wars of choice rather than existential peer-level conflict – in essence, the UK has been preparing for the wrong kind of war.

Meanwhile, despite the geographical advantages inherent to the UK, the infrastructure enabling effective logistics is in fact significantly limited. With most military

maritime embarkation occurring through the Marchwood Sea Mounting Centre, and strategic lift and air-to-air refuelling largely operating from RAF Brize Norton, the UK is reliant on a small number of relatively vulnerable and exposed locations to provide strategic support to Alliance forces (e.g. through deployment of the ARRC), as illustrated in Figure 13.

Figure 13: Selected examples of core UK Defence sites



SOURCE: RAND Europe analysis.

2.10.2. What can the UK do about it by 2030?

The efforts of Ukraine to resist and fight the Russian invasion could hold several lessons for the UK in terms of its future force structure and building a resilient and adaptable military capable of carrying out priority strategic tasks while retaining the ability to absorb losses in a long war and maintain operational viability. Key considerations include:

- **Prepare for attrition by integrating affordable precision mass.** The three armed forces services are already moving towards this solution, with future operating concepts like the Army's 20:40:40 model, the Hybrid Navy or the RAF's Collaborative Combat Aircraft indicating a shift in thinking to include cheap uncrewed mass in a new, more balanced force structure. However, there are a huge number of moving parts to consider in such a shift – including potential changes to doctrine (e.g. precision over saturation), technological integration and interoperability challenges, and a recalibration of policy to enable innovation and adaptation in delivering a new kind of capability.[52]
- **Explore options to improve survivability.** Exquisite capability will maintain a central role in contemporary and future warfare, and the UK's strategic capabilities will remain a core pillar of its force offer to NATO. However, in the context of a peer-level European conflict, increasing the survivability of these platforms is crucial. The UK should learn lessons from the innovative approaches of its allies and partners – for example, the USAF's Agile Combat Employment for air operations, or the dispersed basing concepts used by the Finnish and Swedish militaries.[53]
- **Ensure survival of lessons as well as platforms.** The importance of embedding continuous learning from frontline experiences into militaries is proven not just historically (e.g. with the most successful US pilots in the Second World War being pulled from the frontline to become instructors) but also more recently in Ukraine, where lessons from the battlespace are being constantly applied for innovation and adaptation. The UK should explore potential mechanisms to embed organisational learning into its military culture – balancing the need for experienced and successful personnel at the frontline with the longer-term imperative to utilise their experience to spread lessons throughout the armed forces and train their successors to fight, survive and win.[54]
- **Identify and invest in suitable redundancies to minimise the impact of disruption to key locations.** There is no easy solution for the UK's reliance on its small number of military ports and airports. Beyond the obvious need to harden these sites (see Air Defence vignette), dispersal is one option – utilising civil infrastructure to increase both survivability and optionality. However, this would be complex and expensive to implement. For example, arranging frameworks to allow naval vessels access to commercial ports might be possible, but constraints like explosives handling regulations complicate matters. The UK should explore options to diversify its embarkment and airlift options and consider whether other options, such as pre-positioning more equipment and personnel forward in Europe, or commercial solutions, might be more suitable in the short-term.

2.11. Vignette 11: Maintaining deterrence and escalation management

May 2030

Upon the outbreak of war, NATO attempts to stick closely to its theory of victory, with forces attempting to fix Russian formations and 'block' further advance into Allied territory. However, with dense Russian integrated air defence systems extending over Estonian airspace and long-range Russian fires holding much of the wider region at risk, NATO is unable to secure freedom of manoeuvre or air superiority. As Russian forces continue to enter Allied territory, it becomes clear that NATO will not be able to rapidly push Russian forces back out of Estonian territory.

As a result, NATO turns to the 'break' element of the theory of victory, launching precision deep strikes against key military targets in Kaliningrad, Belarus and the Western Military District to collapse Russian defences. C2 nodes, logistical hubs and munitions depots are key targets, with the overarching objective of the campaign to break the Russian ability to fight and thus secure an operational victory in Estonia. The campaign continues through the war, but despite relatively frequent tactical successes, the strikes do not appear to have the desired political effect in Russia.

Meanwhile, Russia launches its strategic operation to destroy critically important targets (SODCIT campaign) across European Allies, including the UK. With key military sites – including strategically significant hubs like the Marchwood Sea Mounting Centre and RAF bases – heavily impacted, the UK and its NATO Allies begin to consider what other Russian assets they might be able to hold at risk to force Russia towards a more limited implementation of SODCIT, whilst minimising the risk of inadvertent escalation.

June 2030

As NATO strikes continue into Russia and Kaliningrad, Russian rhetoric escalates rapidly, with the president and his ministers regularly issuing increasingly explicit nuclear threats against the NATO Allies involved in these strikes. For now, leaders in the UK remain relatively unconcerned; the UK reminds Russia that they have nuclear weapons as well and will use them in response to any nuclear attack on an Ally, while the UK continues to coordinate closely on nuclear matters with France, the United States and NATO.

September 2030

Military commanders in the Baltics are concerned when satellite ISR picks up movement of suspected tactical Russian nuclear warheads to forward bases, where it is believed they are being coupled with dual-capable delivery systems. Unsure of which systems might be nuclear, NATO commanders restrict strikes on bases suspected of hosting the warheads to avoid any potential catastrophic escalation.

Meanwhile, the Russian defence minister announces that Russia has mobilised tactical nuclear forces and is willing to use them in defence of Russian lives and territory. This causes decision paralysis among decision makers at the highest level in the UK and at NATO, who find themselves with no credible options to respond without triggering an unpredictable escalation spiral. Fear and panic set in at the prospect of genuine Russian nuclear use, and some in the UK, worried that Russian nuclear use would prioritise the UK, begin to call for a halt to UK contributions to strikes into Russia and even for the pulling back of troops from the frontline.

2.11.1. What is the broader problem?

As per NATO's public theory of victory (as of October 2026), the aim in a large, peer-level conflict is to block, blunt and if necessary break the enemy's warfighting system, with the latter step using both long-range precision strikes and cheap mass effectors to target C2 nodes, logistics hubs and any relevant enablers.[55] In practice, it is feasible (if not almost certain) that this would involve strikes within both the Kaliningrad exclave and Russia proper, yet NATO has been clear that the Alliance would not seek to impose strategic defeat upon an adversary. The problem is that the longer a war, the more likely that under-pressure Russian leadership employs more extreme signals and escalates at the strategic level. Ultimately, it is unclear how the UK (and NATO, without the United States) can fight and win a conventional war without risking triggering (potentially nuclear) escalation – the core question is therefore how to signal to Russian leadership that they can lose a conventional war operationally and tactically while surviving a NATO victory.

As for the UK itself, despite being just one of two nuclear-armed states in Europe (the other being France), it has no articulated 'vision' of what intra-war deterrence looks like – at least, certainly not within the public domain. The UK relies entirely on the CASD (so, a single leg of the nuclear triad), which in reality means that it is configured for strategic deterrence, but not necessarily anything else. CASD is designed to remain hidden – which makes it almost impossible to use as a tool for signalling below the very highest level of deterrence. Meanwhile, in the global balance of nuclear weapons and, in particular, the balance of tactical nuclear weapons, the UK (and indeed, France) is vastly outmatched (see Figure 14).

Ultimately, it is unclear how the UK (and NATO, without the United States) can fight and win a conventional war without risking triggering (potentially nuclear) escalation – the core question is therefore how to signal to Russian leadership that they can lose a conventional war operationally and tactically while surviving a NATO victory.

Figure 14: Size of the Strategic and Tactical Nuclear Arsenals of NATO Allies and Russia



SOURCE: Eken et al. 2025.

This should be concerning because in a drawn-out conventional war, especially one involving potential strikes within Russia itself, escalation including strong nuclear signalling is extremely likely – the Russian conceptualisation of deterrence encompasses the employment of nuclear threats and movement/deployment of nuclear capability to shape behaviour and manage escalation.[56] For the UK, this would rapidly become problematic because it has more limited options – or 'rungs' on the escalation ladder – to respond.

2.11.2. What can the UK do about it by 2030?

The coordination of nuclear capability for deterrence across Europe is a live, ongoing conversation between the UK, France and other NATO Allies. There is no easy answer, but the UK and the Alliance may be able to take

some shorter-term steps and at least increase their understanding of the threat and what might be required to deal with it:

- **Harden critical targets and demonstrate Alliance cohesion and strength.** A strong deterrent posture pre-war may well deter such a scenario in the first place. NATO can achieve this by demonstrating to Russia that it is ready and willing to fight and win a long war if it needs to. This will involve many of the same steps discussed in the vignettes above – including investment in effective IAMD to minimise the impact of a potential Russian SODCIT campaign and building resilience across Defence, industry and the public.
- **Simulation and gaming to understand escalation dynamics.** These kinds of exercises are not predictive but can help decision makers to understand and analyse Russian escalation management and the dynamics at play – while also preparing decision makers to handle the extreme pressures of such a scenario and avoid decision paralysis exactly when decisiveness is required most.[57]
- **Embed escalation sensitivity into military planning and campaign design.** With an understanding of Russian strategic culture, an awareness of how strategic and operational choices might inadvertently feed into escalation spirals – and how to handle them when they do occur – can be promoted among UK decision makers and military commanders. Meanwhile, tools like military-to-military comms channels should be implemented and preserved even in crisis to provide pathways for communications on thresholds and red lines.[58]

2.12. Vignette 12: War termination and post-war security architecture

November–December 2030

Seeking to bring an end to active warfighting – and in particular, strikes onto home soil – the UK and other Western European states agree ceasefire terms with Russia. Driven to stop kinetic action as soon as possible, the text of the ceasefire agreement is left ambiguous across several elements – including a lack of precise geographic coordinates for a demilitarised zone (DMZ) either side of the current line of contact, no clarity over the conditions and procedures for withdrawing weapons, and unclear sequencing over the order of ceasefire implementation steps that may be conditional upon the completion of others.

European Allies set up and deploy the Baltic Reassurance Force (BRF), a multinational force of roughly 80,000 troops centred around a land component with supporting air and maritime capability. The force is led by the UK, France and Germany, with contributions from 12 other Allies in Eastern and Central Europe. The BRF's objectives are to maintain the terms of the ceasefire agreement and deter any further Russian military aggression in the region.

January 2031 onwards

Almost immediately, the boundaries of the ceasefire are tested. Russian forces drag out the process of retreating from the DMZ, including failure to remove heavy weapons. Allied leaders press the Russian president on these incidents during peace talks but are rebuffed with claims that Russian forces are adhering to the terms and geographical limits set out in the ceasefire, pointing to the vague terms

of the deal. Western leaders know that Russia is not behaving in the spirit of the deal but reluctantly acquiesce, with no stomach to resume full-scale warfighting.

The BRF soon encounters resistance, including hybrid activities, cyberattacks and sabotage of the BRF's deployed infrastructure, and several standoffs with Russian military formations in the proposed DMZ. The outbreak of fresh violence is largely prevented, but the BRF is reactively pulled in multiple directions, and its operations look increasingly ad hoc and incoherent. Further complications arise after a standoff between the BRF and Russian forces where several weapons are discharged. In response, some contributing states announce that their forces' involvement in the BRF mission is now subject to national caveats around their rules of engagement. Without agreed coordinated response measures and common rules of engagement, the BRF struggles to maintain its credibility in the face of increasingly bold Russian activity probing the limits of the ceasefire.

2.12.1. What is the broader problem?

Designing – and more importantly, effectively implementing – a ceasefire and peace plan is an enormously complex and challenging task. There is huge uncertainty about what a post-war settlement – whether in the context of Ukraine or another potential future war in Europe – could or should look like. When active warfighting ends, the book does not close on a conflict. The political-military settlement, economic recovery, humanitarian aid and beyond are all just as important but are often sidelined when it comes to discussions of future war in Europe in favour of first figuring out how to win on the battlefield. As a result, the question of what comes next remains unresolved. Part of the problem is that planning for a post-war settlement involves planning for unknown quantities. In particular, there are serious questions to consider over how a war ends and what implications that might have for Russia – whether that be a collapse of the regime and the unpredictable political and societal fallout thereof or a continuation of a regime that has demonstrated itself to be both willing and capable of extreme aggression in Europe (as illustrated in the above vignette). Either of these pathways would have severe implications for the UK and its allies – but the problems and risks involved are not well understood. Without a sense of the desired end-state and how to get there, generating genuine post-war security could prove as challenging a test as the conflict itself.

2.12.2. What can the UK do about it by 2030?

There are no clear solutions to this problem, given the vast scope and infinite pathways a conflict scenario and post-war efforts at peacebuilding could take. Solutions would of course need to be bespoke to the specific actors and events in question. However, addressing this problem is more about considering how to approach unresolved questions rather than coming up with specific resolutions that may not be applicable.

- **Start thinking about post-war security architectures now.** Consideration of what long-term peace should look like at a broader level, rather than achieving war termination alone, will be a long-term effort. Rather than conducting ceasefire and peace talks under pressure – generally leading to imperfect and unstable outcomes – the UK and NATO Allies should invest time and resources in developing a coordinated, coherent plan to approach

talks long before negotiations (and potentially even hostilities) begin.

- **Be explicit about potential responsibilities and mechanisms.** RAND research has found that core issues that often lead to the failure of ceasefires and peace treaties include: ambiguity about roles, responsibilities and requirements (which enables misinterpretation, deliberate or otherwise); the absence of robust accountability mechanisms (which enables consequence-free violation); and failure to address the underlying drivers of conflict, and rigidity in terms (which fails to provide for adaptation should it become clear that effective implementation of the original terms is unlikely). These do not represent predictive problem-solving, which may backfire and fail, but core principles which should guide current and future thinking about post-war security.

3. Conclusions

The hypothetical vignettes set out in this paper are not meant to predict the events of 2030. They represent a consciously provocative version of one of the infinite pathways that the UK's (and Europe's) future security could take – they are an illustrative, not predictive, vision of the future. What these vignettes do represent, however, is the diverse range of urgent problems facing defence, security and resilience planning. None have easy solutions, especially in the context of enduring resource constraints, and none can be properly addressed by government alone. At the very least, the UK and likeminded NATO Allies need to be talking about and planning for these issues to ensure that the right mechanisms can be put in place by the time they might be needed in wartime.

To be clear, this scenario is designed to demonstrate not that the UK is doomed to failure in a conflict. Rather, it needs to bolster its ability to deal with shocks – whether that be a war, a pandemic, a natural disaster or something else entirely. The overarching lesson should not be a checklist to prepare for war but the understanding that the machinery of government and models for engagement with industry and society must evolve to deal with the myriad complex pressures of a major interstate war in the 21st century. This is not just a Defence or a government responsibility but a cross-societal one to consider what shocks the UK might be subject to in the future, plan for and build resilience to them, and ultimately attempt to deter and prevent them by showing to adversaries a seriousness and an urgency in preparing for the worst.

Notes

[1] Eken et al. (2025).

[2] Kreetz et al. (2025).

[3] MOD (2025b).

[4] Caves et al. (2021).

[5] RAND Europe's 2026 publication *Strengthening UK National Resilience and Warfighting Readiness: Pragmatic Applications of Swedish Total Defence Concepts and Policies*.

[6] Nicholson et al. (2021).

[7] Caves et al. (2021).

[8] RAND Europe's 2026 publication *Strengthening UK National Resilience and Warfighting Readiness: Pragmatic Applications of Swedish Total Defence Concepts and Policies*.

[9] Caves et al. (2021).

[10] Caves et al. (2021).

[11] RAND Europe's 2026 publication *Strengthening UK National Resilience and Warfighting Readiness: Pragmatic Applications of Swedish Total Defence Concepts and Policies*.

[12] Kreetz et al. (2025).

[13] Muravska et al. (2021).

[14] Lucas et al. (2024).

[15] Department of Health and Social Care (2025).

[16] Kreetz et al. (2025); Van Soest et al. (2025).

[17] Van Soest et al. (2025).

[18] Van Soest et al. (2025).

[19] Van Soest et al. (2025).

[20] Van Soest et al. (2025).

[21] Van Soest et al. (2025); Mcfarlane & Slattery (2026).

[22] Symonds (2026).

[23] NHS Employers (2021).

[24] NAO (2020).

[25] Arnold & Horne (2026); Lynn & Menon (2024).

[26] Abdurasulov (2026).

[27] Arnold & Horne (2025).

[28] Arnold & Horne (2025).

[29] NAO (2020).

[30] Walsh et al. (2026).

[31] Piesing (2026).

[32] Samson & Brett (2026).

[33] Suess (2026).

[34] Retter et al. (2022).

[35] Retter et al. (2022).

[36] MOD (2023a).

[37] Retter et al. (2025).

[38] Retter et al. (2025); Fay (2026).

[39] Fay (2026).

[40] Fay (2026).

[41] Retter et al. (2025).

[42] Mann et al. (2022).

[43] NAO (2025).

[44] MOD (2023b); MOD (2025a).

[45] Kreetz et al. (2025).

[46] Kreetz et al. (2025).

[47] Kaushal (2025).

[48] Black & Dee (2026).

[49] Dee et al. (2025a).

[50] Wachs (2023).

[51] Norsk Luftvern (2025).

[52] Black et al. (2024).

[53] Solli et al. (2022).

[54] Dee et al. (2025b).

[55] NATO (2026).

[56] Eken et al. (2025).

[57] Eken et al. (2025).

[58] Van Hooft et al. (2026).

References

Abdurasulov, Abdujalil. 2026. '"I ran because I knew I would die": Russian drones target medics in Ukraine.' BBC News, 8 August. As of 20 October 2026: https://www.bbc.co.uk/news/articles/c3r073eqvrjo

Arnold, Ed & Si Horne. 2025. 'European Medical Provision in Times of War.' RUSI.org, 6 October. As of 20 October 2026: https://www.rusi.org/explore-our-research/publications/commentary/european-medical-provision-times-war

Barry, Ben, Jonty Kennon, Douglas Barrie, Nick Childs, James Hackett, Henry Boyd, Jonathan Bentham, Dzaky Naradichiantama & Michael Tong. 2025. *A European Reassurance Force for Ukraine: Options and Challenges.* International Institute for Strategic Studies. As of 20 October 2026: https://www.iiss.org/research-paper/2025/03/a-european-reassurance-force-for-ukraine--options-and-challenges/

Beraud-Sudreau, Lucie. 2026. 'Defence supply chains beyond CRMs: dependencies and bottlenecks.' International Institute for Strategic Studies, Military Balance Blog. As of 20 October 2026: https://www.iiss.org/online-analysis/military-balance/2026/05/defence-supply-chains-beyond-crms-dependencies-and-bottlenecks/

Black, James, Pauline Paille, Charlotte Kleberg, Conlan Ellis & Maxime Sommerfeld Antoniou. 2024. *Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine*. Santa Monica, Calif.: RAND Corporation. RR-A3400-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA3400-1.html

Black, James & Stuart Dee. 'Bringing Directed Energy Weapons Into Focus: Integrating Emerging Capabilities Into NATO Air Defence.' *The Journal of the JAPCC (Joint Air Power Competence Centre)*, 42, 38-45. As of 20 October 2026: https://www.rand.org/pubs/external_publications/EP71509.html

Braw, Elizabeth. 2025. 'Financial institutions should prepare for subsea cable sabotage.' Financial Times, 14 July. As of 20 October 2026: https://www.ft.com/content/cf16a5b4-6961-4b6c-80fb-6238b73338bd

BBC. 2017. 'Could Russia cut undersea communication cables?' BBC News, 15 December. As of 20 October 2026: https://www.bbc.co.uk/news/world-42365191

Caves, Ben, Rebecca Lucas, Livia Dewaele, Julia Muravska, Chris Wragg, Tom Spence, Zudik Hernandez, Anna Knack & James Black. 2021. *Enhancing Defence's Contribution to Societal Resilience in the UK*. Santa Monica, Calif.: RAND Corporation. RR-A1113-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA1113-1.html

Dee, Stuart, Katja Fedina, Kiran Suman-Chauhan, Evie Graham, Daniel Hill, Andrew Gibson, John Kendall & John Foreman. 2025a. *Invisible Defender? Opportunities and Challenges for Integrating DEWs into Ukraine's C-UAS Framework*. Santa Monica, Calif.: RAND Corporation. RR-A3833-7. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA3833-7.html

Dee, Stuart, Katja Fedina, Kiran Suman-Chauhan, Evie Graham, Daniel Hill, Andrew Gibson, John Kendall & John Foreman. 2025b. *Lessons Learned: Understanding the Role of Military Organisational and Adaptation Culture for the Future of Ukraine's Defence*. Santa Monica, Calif.: RAND Corporation. RR-A3833-5. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA3833-5.html

Department of Health & Social Care. 2025. *Managing a robust and resilient supply of medicines*. GOV.UK. As of 20 October 2026: https://www.gov.uk/government/publications/managing-a-robust-and-resilient-supply-of-medicines/managing-a-robust-and-resilient-supply-of-medicines#the-uk-medicines-supply-chain

Edwards, Charlie & Nate Seidenstein. 2025. *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. International Institute for Strategic Studies. As of 20 October 2026: https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure

Eken, Mattias, Kiran Suman-Chauhan, Beatrice Aubert & Paul van Hooft. 2025. *Understanding Russian Strategic Culture and the Low-Yield Nuclear Threat*. Santa Monica, Calif.: RAND Corporation. RR-A3859-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA3859-1.html

Fay, Joe. 2026. 'How the defence sector is battling a skills crisis.' BBC News, 2 January. As of 20 October 2026: https://www.bbc.co.uk/news/articles/clyd1lpp1lyo

Finnish Government. 2025. *Security Strategy for Society: Government Resolution*. As of 20 October 2026: https://julkaisut.valtioneuvosto.fi/items/0126122a-1e8a-4ffa-9868-6286292efc01

Finnish Ministry of the Interior. 2025. 'Baltic Sea countries to intensify cooperation in countering hybrid threats.' Valtioneuvosto.fi, 28 October. As of 20 October 2026: https://valtioneuvosto.fi/en/-/1410869/baltic-sea-countries-to-intensify-cooperation-in-countering-hybrid-threats

Geiger, Chas. 2024. 'UK armed forces not ready for high-intensity war, MPs warn.' BBC News, 4 February. As of 20 October 2026: https://www.bbc.co.uk/news/uk-politics-68181275

Hall, Ben & Madeleine Speed. 2026. 'NATO should prepare for deadly Russian "hybrid" attack, says Poland.' Financial Times, 12 October. As of 20 October 2026: https://www.ft.com/content/0c5a10f4-5aca-456e-9c3a-4c4dc8132a63?syn-25a6b1a6=1

Kaushal, Sidharth. 2025. *An Integrated Air and Missile Defence Architecture for the UK*. RUSI Occasional Papers. As of 20 October 2026: https://www.rusi.org/explore-our-research/publications/occasional-papers/integrated-air-and-missile-defence-architecture-uk

Kreetz, Tristan, Judith Huismans, Fook Nederveen, Conlan Ellis & Francesca Ghiretti. 2025. *Netherlands Prepared: Lessons from war economies for a resilient society*. Santa Monica, Calif.: RAND Corporation. RR-A4063-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA4063-1.html

Lanaute, Thomas. 2023. 'Navigating the Underwater Threat: Risks of Subsea Cable Disruptions for Financial Services.' BSO.co, 1 June. As of 20 October 2026: https://www.bso.co/all-insights/mitigate-risk-of-subsea-cables-disruptions-finacial-services

Lucas, Rebecca, Thomas Ekstrom, Paola Fusaro, Elizabeth Hastings Roer & Lucia Retter. 2024. *Toward Defense Supply Chain Disruption Management: A Research Agenda for Defense Supply Chain Resilience*. Santa Monica, Calif.: RAND Corporation. RR-A2504-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA2504-1.html

Lynn, Guy & Stephen Menon. 2024. 'Fix NHS gaps or face more attacks – ex cyber chief.' BBC News, 8 July. As of 20 October 2026: https://www.bbc.co.uk/news/articles/czd9glyx414o

Mann, Bruce, Kathy Settle & Andy Towler. 2022. *Independent Review of the 2004 Civil Contingencies Act*. National Preparedness Commission. As of 20 October 2026: https://nationalpreparednesscommission.uk/publications/independent-review-of-the-2004-civil-contingencies-act/

Mcfarlane, Sarah & Gram Slattery. 2026. 'NATO allies foil Russian subsea cable sabotage plot.' Reuters, 10 September. As of 20 October 2026: https://www.reuters.com/world/europe/nato-allies-foil-russian-subsea-cable-sabotage-plot-2026-09-10/

Ministry of Defence (MOD). 2023a. *Agency and Agility: Incentivising people in a new era – a review of UK Armed Forces incentivisation*. As of 20 October 2026: https://www.gov.uk/government/publications/agency-and-agility-incentivising-people-in-a-new-era-a-review-of-uk-armed-forces-incentivisation

———. 2023b. 'Ministry of Defence – Commercial X.' Ministry of Defence, 15 August. As of 20 October 2026: https://www.gov.uk/guidance/ministry-of-defence-commercial-commercial-x

———. 2025a. *Defence Industrial Strategy 2025: Making Defence an Engine for Growth*. As of 20 October 2026: https://www.gov.uk/government/publications/defence-industrial-strategy-2025-making-defence-an-engine-for-growth

———. 2025b. *The Strategic Defence Review 2025 – Making Britain Safer: Secure at home, strong abroad*. As of 20 October 2026: https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad

Muravska, Julia, Anna Knack, Rebecca Lucas & Ben Williams. 2021. *Challenges and Barriers that Limit the Productivity and Competitiveness of UK Defence Supply Chains*. Santa Monica, Calif.: RAND Corporation. PE-A117-1. As of 20 October 2026: https://www.rand.org/pubs/perspectives/PEA117-1.html

National Audit Office (NAO). 2020. *The supply of personal protective equipment (PPE) during the COVID-19 pandemic*. As of 20 October 2026: https://www.nao.org.uk/wp-content/uploads/2020/11/The-supply-of-personal-protective-equipment-PPE-during-the-COVID-19-pandemic.pdf

———. 2025. *The UK's F-35 capability*. As of 20 October 2026: https://www.nao.org.uk/reports/the-uks-f-35-capability/

———. 2026. *Resilience of the food supply chain to disruptions*. As of 20 October 2026: https://www.nao.org.uk/wp-content/uploads/2026/09/Resilience-of-the-food-supply-chain-to-disruptions.pdf

NATO. 2026. 'SACEUR's Remarks at the Warsaw Security Forum.' SHAPE.NATO.INT. As of 20 October 2026: https://shape.nato.int/page11283634/speeches-and-transcripts/saceurs-remarks-at-the-warsaw-security-forum.aspx

Navy Lookout. 2026. 'Royal Navy Attack Submarine Fleet Update – All Boats Alongside.' Navylookout.com, 25 June. As of 20 October 2026: https://www.navylookout.com/royal-navy-attack-submarine-fleet-update-all-boats-alongside/

NHS Employers. 2021. *Key Facts About Employing Reservists in the NHS*. NHSemployers.org. As of 20 October 2026: https://www.nhsemployers.org/system/files/2021-07/Key-facts-about-employing-reservists-in-the-nhs_0.pdf

Nicholson, Joanne, Peter Dortmans, Marigold Black, Marta Kepe, Sarah Grand-Clement, Erik Silfversten, James Black, Theodora Ogden, Liva Dewaele & Pau Alonso Garcia-Bode. 2021. *Defence Mobilisation Planning Comparative Study*. Santa Monica, Calif.: RAND Corporation. RR-A1179-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA1179-1.html

Norsk Luftvern. 2025. 'The European Sky Shield Initiative (ESSI).' Norskluftvern.com, 21 July. As of 20 October 2026: https://norskluftvern.com/2025/07/21/the-european-sky-shield-initiative-essi/

Piesing, Mark. 2026. 'Satellite killers: What a war in space might look like.' BBC Future, 31 July. As of 20 October 2026: https://www.bbc.co.uk/future/article/20260730-satellite-killers-what-a-war-in-space-might-look-like

Reach, Clint, Alexis A. Blanc & Edward Geist. 2022. *Russian Military Strategy: Organizing Operations for the Initial Period of War*. Santa Monica, Calif.: RAND Corporation. RR-A1233-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA1233-1.html

Retter, Lucia, Zsofia Wolford, Nicolas Jouan, Stella Harrison, Charlotte Kleberg & Melusine Lebret. 2025. *Maritime Skills on the Clyde: Demand, supply and options for supporting skills growth*. Santa Monica, Calif.: RAND Corporation. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA3558-1.html

Retter, Lucia, James Black & Theodora Ogden. 2022. *Realising the Ambitions of the UK's Defence Space Strategy: Factors Shaping Implementation to 2030*. Santa Monica, Calif.: RAND Corporation. RR-A1186-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA1186-1.html

Samson, Victoria & Kathleen Brett (eds.). 2026. *2026 Global Counterspace Capabilities Report*. Secure World Foundation. As of 20 October 2026: https://www.swfound.org/publications-and-reports/2026-global-counterspace-capabilities-report

Solli, Per Erik, Robin Haggblom & Anders Persson. 2022. 'A Flexible and Resilience Nordic Air Base Concept.' *Luftled*, 3 December. As of 20 October 2026: https://luftled.info/a-flexible-and-resilient-nordic-air-base-concept/

Suess, Juliana. 2026. 'Checkmate? Russian Orbital Manoeuvring Threatens Ukraine's Space Capability.' RUSI.org, 17 June. As of 20 October 2026: https://www.rusi.org/explore-our-research/publications/commentary/checkmate-russian-orbital-manoeuvring-threatens-ukraines-space-capability

Symonds, Tom. 2026. 'Iran-linked hackers behind cyber attack that shut down power plant, reports say.' BBC News, 23 August. As of 20 October 2026: https://www.bbc.co.uk/news/articles/ce9793g34yvo

UK Space Agency, Department for Business, Innovation, Science and Trade & Ministry of Defence. 2026. *UK Space Strategy*. As of 20 October 2026: https://www.gov.uk/government/publications/uk-space-strategy

van Hooft, Paul, Mattias Eken, Zsofia Wolford, Artur Honich, Thomas Kenchington & Kiran Suman-Chauhan. 2026. *Conventional Logics, Nuclear Fears: Inadvertent Escalation Risks Between NATO and Russia*. Santa Monica, Calif.: RAND Corporation. RR-A4739-1. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA4739-1.html

van Soest, Henri, James Black, Harper Fine & Lucia Retter. 2025. *Evolving Threats to Critical Underwater Infrastructure: Implications for European Security and Resilience*. Santa Monica, Calif.: RAND Corporation. PE-A3800-1. As of 20 October 2026: https://www.rand.org/pubs/perspectives/PEA3800-1.html

Wachs, Lydia. 2023. *Russian Missiles and the European Sky Shield Initiative*. SWP Comment, No. 45, August 2023. As of 20 October 2026: https://www.swp-berlin.org/publications/products/comments/2023C45_european_sky_shield_initiative.pdf

Walsh, Stephanie J., Marta Kepe, Salman Ahmed, Barbara Del Castello, Matt Chessen, Marzia Giambertoni, Cian Girven, Richard S. Girven, Theiline Pigott & Anton Shenk. 2026. *Infinite Potential – Insights from the European Games: After-Action Report from a Sequence of Day After Artificial General Intelligence Exercises*. Santa Monica, Calif.: RAND Corporation. RR-A4767-2. As of 20 October 2026: https://www.rand.org/pubs/research_reports/RRA4767-2.html

Webster-Smith, Richard & Emma Black. 2025. 'Shifting UK attitudes on defence.' FGS Global, 14 April. As of 20 October 2026: https://fgsglobal.com/insights/shifting-uk-attitudes-on-defence

About this paper

In the context of Russia's war of aggression in Ukraine and an intensification of its subthreshold operations against the UK and its NATO Allies, there is now a credible threat of peer-level conflict in Europe by 2030. It is no longer a question of whether a war is possible, but whether we are prepared to fight one. In this paper, the authors examine a range of different potential dimensions to an illustrative hypothetical future NATO-Russia war, including the threats posed, the broader problems these threats represent, and potential means to mitigate or prevent them.

About the authors

James Black is deputy director of the Defence, Security and Justice research group at RAND Europe. His research focuses on the future of strategic competition, deterrence and warfighting and the impact of emerging technologies, including nuclear, AI and space. James is also Lead of the RAND Europe Space Hub.

Kiran Suman-Chauhan is an analyst at RAND Europe. Working within the Defence, Security and Justice team, his work sits at the intersection of defence capability, industry and emerging and disruptive technologies. Kiran's recent work encompasses capability and technology assessment, analyses of national defence industrial bases, and explorations of the impact of emerging technologies including AI-enabled systems and directed-energy weapons on military operations and strategy.

Leanne Iorio is an analyst in the Defence, Security and Justice research group at RAND Europe. Her research primarily focuses on NATO strategy and Alliance dynamics; the challenges and opportunities presented by emerging and disruptive technology, evolving AI technologies, and the cyber domain; and wargaming approaches to understanding defence, deterrence, and multilateral decision-making in complex global and national security environments.



PE-A5505-1