JUNE 2024

BENEDICT MACON-COONEY
AMALIA KHACHATRYAN
MELANIE GARSON
JEEGAR KAKKAD
DANIEL SLEAT
LUKE STANLEY
JARED WRIGHT
KEVIN ZANDERMANN

Reimagining Defence and Security: New Capabilities for New Challenges

TONY BLAIR INSTITUTE FOR GLOBAL CHANGE

Contents

Our Future of Britain initiative sets out a policy agenda for governing in the age of AI. This series focuses on how to deliver radical-yet-practical solutions for this new era of invention and innovation – concrete plans to reimagine the state for the 21st century, with technology as the driving force.

01

Foreword

Decades from now, when historians write about this period, they will undoubtedly characterise today's geopolitical environment as an inflection point – an era when old assumptions gave way to new and uncomfortable realities. The post-Cold War dream of a Europe "whole, free and at peace" has been replaced by a Europe wracked by Russia's war of aggression against Ukraine. The notion that a rising China, once fully integrated into the global economy, would become a "responsible stakeholder" in the rules-based international order has been overtaken by a revisionist China that is willing to use coercive measures, including military force, to try to unilaterally change the status quo in the Asia-Pacific. Previously unimagined alliances, like that between Russia, China, Iran and North Korea, are forming as old partnerships weaken and more countries in the Global South become "swing states" whose allegiances shift depending on the issue and situation. What's more, the baseline assumption that the United States and its European allies would remain fully engaged in the world is now challenged by political leaders in almost every country.

But that's not all. Further complicating matters is the persistence of perennial threats like terrorism alongside the emergence of serious transnational threats

like climate change and lethal pandemics.

At the same time, the world is experiencing a profound period of technological disruption – with the advent of AI, advances in biotech, quantum technologies, future-generation wireless technologies, advanced materials, new space technologies, hypersonics, directed energy and others – that will have deep impacts on societies and on how militaries deter and fight in the future.

Given this complex, volatile and increasingly dangerous geopolitical context, this paper makes a compelling case for rethinking defence and national-security policy, particularly for middle powers like the UK and many of its European allies. A fresh assessment of strategic priorities and how best to achieve them is essential, along with hard choices about where to accept and manage risk, given that national resources for defence are never unlimited.

Not only does the UK need to rethink strategy, it also needs to rethink how it makes strategy. A more centralised approach that better integrates all of the instruments of national power is critical, as is rethinking how the public and private sectors work together to achieve national objectives. Given the rapid pace of change, the strategy-development process also needs to give the future a larger seat at the table. This paper helpfully recommends several structural innovations to develop more effective and resilient whole-of-nation policies.

While a new UK strategy must reinvest in the drivers of the nation's competitiveness and security, the authors rightly argue that the UK cannot and should not go it alone. The UK's alliances will be central to its success. Therefore, strategy development must be done in close collaboration with NATO and other allies, identifying shared objectives, developing common approaches and coordinating investments to achieve desired outcomes.

This increased collaboration with allies is even more important given how quickly and substantially the ways future wars will be fought (or prevented) are evolving. Virtually every operation will be conducted in alliance or coalition with other like-minded states, and these operational partners must work hard to develop new operational concepts, new technologies to share a common operational picture, and resilient and interoperable C4ISR networks to operate effectively together on a highly contested and lethal battlefield. These innovations, and their adoption, can no longer happen inside national stovepipes; they must be designed to be shared, and where possible co-

developed, with allies from the start.

Unfortunately, as Presidents Putin and Xi have reminded us, time is of the essence. The UK and its allies need to strengthen deterrence by integrating new capabilities and operational concepts now. Adopting innovation with speed and scale is the name of the game. And, as the authors argue, existing approaches to hardware procurement have proven too slow and ill adapted for acquiring rapidly evolving technologies and software-driven solutions. The reforms they propose, ranging from earlier and deeper engagement with the private sector to better utilisation of tech-savvy specialists within government to drive it, are spot on. All of this has major implications for the type of personnel that need to be recruited, developed and retained in the Ministry of Defence and the armed forces, with new incentives and career paths established to reward and promote those who able to drive innovation adoption.

This paper by the Tony Blair Institute for Global Change sets out some truly fundamental and important questions that any future defence strategy needs to answer, as well as a new model for how such a strategy could be developed in the UK and with key allies. It rightly calls on the broader defence and national-security community to reimagine allied defence strategy given the evolving threat landscape, reconceive of the processes we use to develop strategy, reform the way we procure new capabilities and recruit talent into defence, and rethink our forces and force posture to be able to keep the peace in a more contested and dangerous future security environment. Whether or not one agrees with each and every recommendation, this paper provides timely and invaluable impetus to the defence debate the United Kingdom, the United States and NATO more broadly must have in order to be ready to deter and, if necessary, prevail in future conflict.

Michèle Flournoy

Former US Under Secretary of Defense for Policy

02

Executive Summary

The world is becoming a more dangerous and unpredictable place. Shifting alliances, new geopolitical actors, asymmetric engagement and transnational ideologies exploit, and are exploited by, new and disruptive technologies emerging at an uncontrolled rate.

The result is mounting uncertainty and a fragile world facing growing contention and, increasingly, open conflict. The geopolitical landscape will become even more complex in the coming decade as the technological revolution, politicisation of trade and evolving allegiances make the world a more contested place.

Non-state actors such as Hamas and insurgents in the Sahel continue to pose substantial threats to the safety and stability of the world, and require firm counter-terrorism capabilities, including boots on the ground where necessary, to fight them.

At the same time, Russia's illegal invasion of Ukraine has presaged a return to great-power conflict, something previously thought to have been left behind in the 20th century. This necessitates a radical upgrade in defence capabilities, backed by increased defence spending, even as countries continue to reel from the financial impact of the Covid-19 pandemic.

Meanwhile, technology is rapidly transforming the character of warfare, creating new vulnerabilities such as cyber-attacks on critical infrastructure, empowering non-state actors with greater capabilities and necessitating varied procurement systems for different types of weapons.

This paper is not intended to be a comprehensive review of the UK's national-security capacity, capability and strategy. This must be set after the general election, informed by the Strategic Defence and Security Review that will likely take place. Instead, this paper highlights critical areas of focus for the review to consider, and sets out the actions necessary to achieve a new vision for deterrence and defence for the shifting geopolitical contexts of today and the future. It does so based on five key pillars: strategy, capabilities, procurement, personnel and alliances.

First, **governments must address these changing geopolitical contexts with the right strategic approach**. The complex nature of the security challenges of our time, as well as the capabilities needed to meet them, requires a new approach to developing defence strategy. This must involve better interaction and integration within government and between the armed services. For too long, formulation of the UK's defence strategy has remained siloed within parts of government. A whole-of-government approach, driven by the centre, is needed, and new structures and frameworks must be created to deliver this approach. These include:

- **A new National Security Team in Downing Street.** Comprising individuals from different disciplines, including military and technology experts, this team would set the defence strategy for the country over two-, five- and ten-year horizons. This strategy would be reviewed on an annual basis by a National Security Assessment.
- **A Centre for Strategic Futures.** This team would report into the new National Security Team in Number 10; its focus would be to assess trends and scenarios shaping key areas such as the economy, technology and security over a 20- to 30-year period. The Centre for Strategic Futures would feed into the National Security Team's security and strategy reviews.

Second, **governments must assess the capabilities they need to adapt to the evolving character of conflict**. Emerging hardware capabilities are changing combat; uncrewed systems and software to utilise them have quickly become a critical capability. These new technologies are being integrated with other, sometimes more traditional, capabilities such as boots on the ground. As these capabilities evolve, so too do the countermeasures to stop them. While, at present, expensive missiles are often needed to shoot down cheap drones, countries are seeking to develop new ways to achieve this at a lower cost. The right security strategy will rest on securing the right balance of these kinds of emerging technologies, alongside traditional capabilities. Critical actions include:

- **Working with allies in Europe to plug high-risk capability gaps that would result from diminished US support.** Urgent gaps to address include integrated air and missile defence capabilities, enemy air defence suppression, and destruction capabilities and long-range strike capabilities beyond the 300 km range.
- **Mass producing cheap, easily replaceable drones.** This will support UK

surveillance, propaganda and strike capabilities.
- **Creating a new AI red-teaming group to continually stress-test cyber-vulnerabilities and critical infrastructure**. If necessary, expertise could be drawn from industry, the National Cyber Security Centre and the AI Safety Institute.

Third, **the emergence of these new technologies and capabilities will require totally new procurement techniques, with greater fusion with the private sector**. As Ukraine has shown, technologies do not change warfare in a static way: they are constantly evolving. Adapting to this requires a completely different approach to sharing risks and incentives with the private sector, so that procurement becomes a collective enterprise focused on innovation and development. This means that reforms to procurement and production will be critical. Current procurement processes are costly, slow and lack sufficient innovation, yet the ability to procure and produce at speed, scale and cost is essential to maintaining defence readiness. Our proposals set out the key reforms needed to support MoD procurement and its ability to foster, facilitate and secure new technologies. Specifically, this paper proposes:

- **A new agency to expand industry partnerships.** This body would focus on deepening ties with startups, SMEs and non-traditional contractors, as well as academia, national laboratories and research institutes. It could follow the model of US firm In-Q-Tel, acting as a go-between for small companies and the MoD, and helping smaller companies navigate the procurement process.
- **Expanded MoD innovation hubs.** Funding for both Defence and Security Accelerator (DASA) and jHUB should be increased to no less than £50 million more per annum. A private-sector technologist should be appointed to lead Defence and Security Accelerator (DASA) and elevated to report to the secretary of state for defence. A defence accelerator unit, aimed at quickly scaling and fielding new technologies, should be established and backed by ample funding.
- **A relentless focus on production.** An initiative to scale mass production of low-cost, expendable systems should be established, modelled on the US Replicator Initiative. Building on the NATO Defence Production Action Plan, a new streamlined process focusing on smaller, more frequent contracts should be introduced, involving producers more directly in the NATO standards-development process. At NATO's Defence Innovation

Accelerator for the North Atlantic (DIANA) innovation hub, a "challenge" to increase modular design and the 3D printing of munitions should be set.

Fourth, **these new technologies will require personnel with a new mix of skills**. New technologies are already changing the shape of the Ukrainian armed forces, with a typical assault group of 12 to 16 soldiers now accompanied by a similar number of drone operators. There is a growing need for data engineers, AI, cyber and tech specialists in armed forces across the world. In the event of a war, the UK may need to draw on the skills and experience of army reserves and resilience organisations, and officials in government will need to be prepared to deal with the day-to-day challenges of managing a country at war. To ensure that the UK's armed forces have the right personnel with the right skills, and that the country is prepared for conflict, the following actions must be taken:

- **Reorganising armed-forces training.** All military training must cover basic digital capabilities, and the UK's Defence Cyber Academy should be expanded into a broader Defence Digital Academy. A more holistic approach to assessing medical fitness for service should be designed, to ensure that medical records only exclude those with the most challenging health problems.
- **Exploring ways to boost the pool of skilled people that can be called upon in the event of a serious war.** These include expanding the army reserves or the planned UK Resilience Academy to ensure the UK has skilled civilians that it can draw on in a crisis.
- **Establishing a Wartime Preparation Taskforce.** Modelled on the Vaccine Taskforce, this would prepare plans for the actions that various departments and institutions would need to take in the event of large-scale conventional war. The taskforce's aim would be to produce a comprehensive internal plan, similar to the Government War Book of the Cold War period.

Fifth, in an era where only the US and China can project themselves alone, most other countries will require **the right network of alliances for their security**. The two "super-superpowers" together spend more on defence than the next 38 countries combined. Without the right allies and alliances, the UK will not be able to form the right defence strategy. This will involve cooperation with European allies and the right partnership with the US, as well as a strategic role in alliances such as NATO and critical technology

partnerships such as the AUKUS security agreement between Australia, the UK and the US. To that end, the UK should:

- **Conduct a comprehensive stocktake and refresh of the state of the UK's international alliances.** Led by the National Security Team, this should encompass bilateral, minilateral and multilateral alliances, and include an assessment of where the UK is able to contribute particular strengths, how these can be augmented by allies and what better coordination with these allies could achieve in terms of enhancing the UK's defence strategy.
- **Establish a dedicated alliances and international-partners unit.** This unit, within the National Security Team, should focus on alliances and international partners, to provide ongoing assessment of alliances, the UK's contribution to them and how these could be improved.

In this new age of instability, countries such as the UK must act fast to address both immediate and near-term defence and security challenges. There is a significant possibility that whoever forms the UK's next government will be the first administration since 1945 to have to fight a large-scale war, and the ideas in this paper are designed to help expedite policy decisions around defence. When it comes to getting the UK war-ready, there is not a moment to lose. The same is true of other countries: no government in the world can afford to avoid a complete reappraisal of their national-security capacity, capability and strategy in order to ensure that they are able to adequately deter – and, if necessary, defend against – attacks.

03

Introduction

In an era marked by unprecedented geopolitical shifts and technological revolution, the fabric of global security has changed. The narrative of our time is not one of peace and stability, but of escalating conflicts and emerging threats that challenge the foundations of international order.

Old wars are fought with new capabilities, with the winners of those conflicts the countries best able to integrate and adapt their tools of warfare at speed and under pressure, and industrialise their production at scale.

The world is witnessing the highest number of conflicts since the second world war, with more than 238,000 lives lost in 2023 alone and more than 90 countries involved in some form of external conflict.

The world is also becoming less predictable. The future of geopolitics is increasingly set by countries of no fixed allegiance, with the ability to take advantage of international competition and influence it. These powers will continue to increase their influence to shape outcomes, adding extra complexity and unpredictability to power rivalry. Furthermore, in today's interconnected world, national security encompasses not only military threats but also non-military dimensions such as economic security, energy security, environmental security and digital security. Working with allies – old and new – will require new paradigms.

The geopolitical chessboard has also become more complex. The balance of power has been shifting for years, alliances are in flux and the rules that once governed international relations are dissolving. In this new era of rivalry, nations such as Russia, China, Iran and North Korea pose multifaceted threats, from territorial aggression to space and cyber-warfare, and are openly hostile to the West. Meanwhile, non-state actors and transnational challenges, such as climate change, add layers of complexity to an already volatile landscape.

Simultaneously and reactively, the battlefield has also evolved. Drones, artificial intelligence and next-generation technologies are redefining the character of war. The war between Armenia and Azerbaijan in 2020 demonstrated the overwhelming difference that drones can make in an era of network-centric warfare. With a disjointed and outdated air-defence system, the Armenian

army crumbled under Turkish-made Bayraktar TB2 and Israeli kamikaze drone attacks on its troops and tanks. Ukraine's deployment of drones also initially proved effective against Russia but spurred the development of counter-drone systems, with Russia quickly excelling in electronic warfare tactics and deployment.

As warfare becomes more network-centric and battles are fought on unconventional terrains, the need for a balanced approach to defence, leveraging both orthodox and emerging capabilities, has never been more critical. This requires the right strategy and a whole-of-government approach to assessing and securing capabilities, procurement and skilled personnel – both on and off the battlefield – to deter and defend in the modern era.

04

21st-Century Geopolitics Needs a 21st-Century Defence Strategy

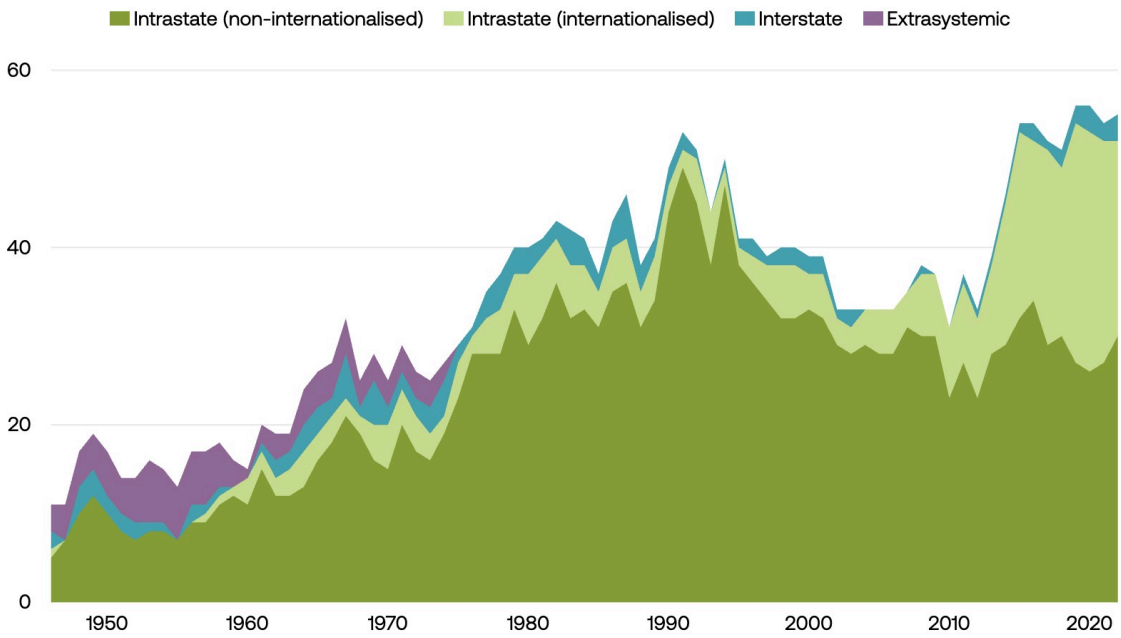
Today's geopolitical trends necessitate a deep rethink of defence policy. We have set out some of these core themes below, as they are important to understand if the right strategy is to be developed.

DEFENCE IN A DANGEROUS AND DIVIDED WORLD

The world is becoming more dangerous, divided and clustered, both in diplomatic and trade terms, around the Global North and South. The two super-superpowers, China and the US, have vast defence budgets, while other powers such as Russia and India have cultivated significant defence purchasing power with smaller budgets.[1] The world is currently experiencing the highest number of conflicts at any point since the end of the second world war, including instability both intrastate[2] and triggered by conflicts in the "grey zone": the contested zone between traditional diplomacy and open conflict.

FIGURE 1

The number of armed conflicts per year is rising

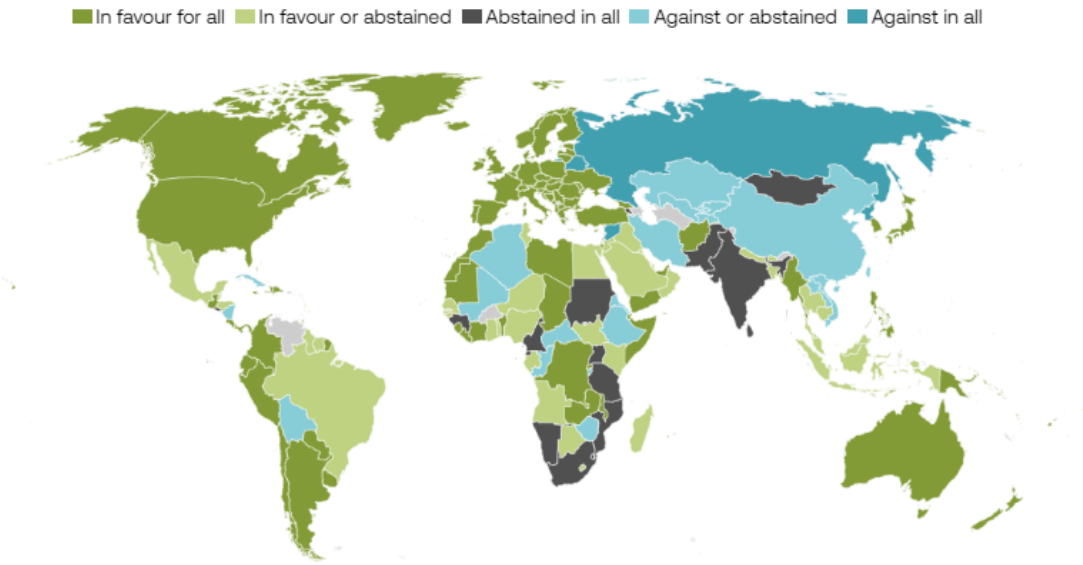


Source: State Street Global Advisors Macro Policy; UCDP via Our World in Data

The global community is increasingly more fragmented and multipolar. In recent years the world has aligned around a more explicit Global North and Global South. The Global South grouping is loosely aligned around China and, to some degree, Russia; the Global North grouping is aligned around the traditional "West", but with only sporadic leadership by the US. This alignment has been visible in voting patterns at the United Nations (UN) General Assembly.[3]

FIGURE 2

Four UN votes condemning Russia's invasion of Ukraine show an increasing divide between a Global North and South



Source: Al Jazeera and United Nations

China, Russia, Iran and North Korea are increasingly working together in an openly hostile coalition to frustrate Western ambitions, exchanging defence technologies and cooperating on ways to blunt Western sanctions.[4] This loose grouping, which some analysts have begun to refer to as CRINK, could increasingly cause problems for the West by raising simultaneous geopolitical crises in different areas of the world.[5] However, while the grouping is loosely framed and transactional in nature, it provides China with considerable weight in global politics, thus making Beijing an important interlocutor for the West, in addition to other Global South coalitions such as BRICS.

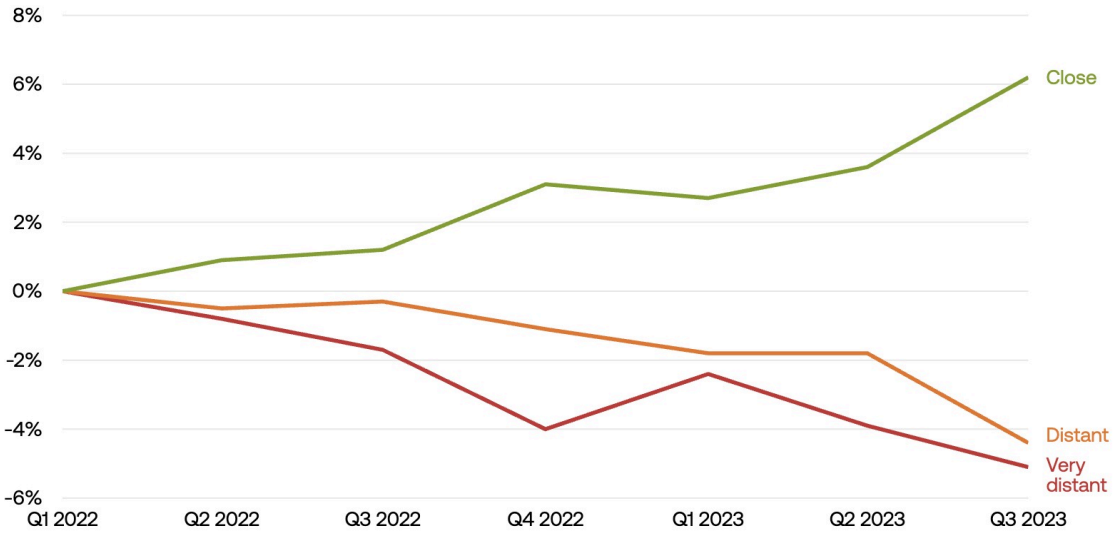
Alongside and around this grouping are multi-aligned states. These states mix occasional issue-based alignment with either the Global North or South with a status that sits outside explicit partnership with either grouping. Turkey, South

Africa, Saudi Arabia and Brazil, for example, sit within this category.

These trends are reflected quite clearly in global trading patterns. Countries are increasingly focusing on trade with geopolitical allies. UN data show that over the past two years there has been a 6 per cent increase in trade between countries considered geopolitical allies and a 4 per cent decrease in trade between countries that are viewed as geopolitically distant.[6]

FIGURE 3

Global trade is increasingly characterised by "friendshoring"

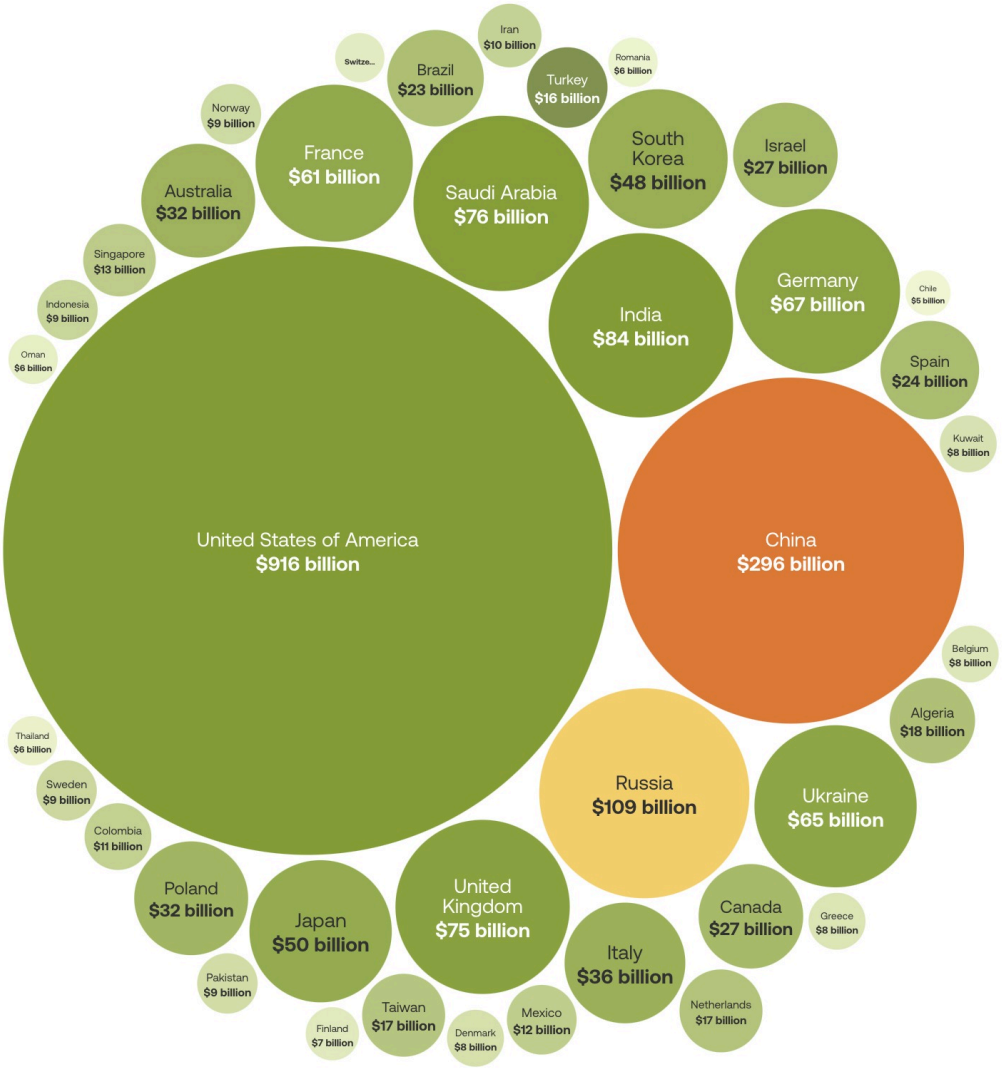


Source: UNCTAD calculations based on global statistics

This constellation is even more complicated in terms of defence spending. Based on Stockholm International Peace Research Institute (SIPRI) data the US and China spend, combined, more on defence than the next 38 countries put together.[7] Within this fragmentation around the world, only the US and China can truly project themselves militarily on a global scale.

FIGURE 4

US and Chinese defence spending dwarfs that of the rest of the world



Source: SIPRI Military Expenditure Database

The future trajectory of China is unclear, and the US's focus, given China's rise, is increasingly turned towards the Pacific. This has important implications for

the UK and Europe.

While former US President Donald Trump's comments on NATO have caused concern about the US's future role in the alliance, they should be a wake-up call – relevant particularly in the context of NATO, but important more widely. The US's commitment to Europe may not be cemented simply by choice but could be driven by events to its west.

NAVIGATING A COMPLEX GEOPOLITICAL AND SECURITY LANDSCAPE

In this context, medium-sized countries such as the UK must give urgent and careful thought to their defence strategies. While Labour's proposed 100-day "security sprint" would help identify emerging and evolving threats, broadly speaking there are four scenarios for which the UK must urgently prepare.

First, Putin's invasion of Ukraine is making the UK's involvement in a large-scale, conventional war in Europe a much more likely scenario than at any time since the end of the Cold War. Various experts have warned that the invasion, and Putin's rhetoric around it, point to wider revanchist ambitions that could lead to further Russian attacks on sovereign European countries. In response to this, the government will need to prepare for scenarios in which Europe has to defend itself from Russian aggression with diminished support from the US, if US forces are committed in the Indo-Pacific. Given the time it can take to move a capability from idea to deployment, train personnel, and reboot stockpiles and the defence industry, the UK has a very narrow window of opportunity in which to prepare for a potential war with Russia. Swift action in the months after the general election will be critical. **Ensuring that UK armed forces are capable of deterring and, if necessary, defending against a Russian attack on NATO must be the most urgent defence priority of the new government.**

Second, advances in technology are increasing the likelihood of unconventional warfare techniques being deployed against Britain through hybrid warfare. The West is becoming increasingly dependent on new forms of infrastructure, such as satellites and undersea cables; these make tempting targets for adversaries, who could carry out physical attacks or sophisticated cyber-attacks.

Third, geopolitical instability is making it more likely that further conflicts will break out without the UK's direct involvement, **but where it has a clear**

strategic or humanitarian reason to provide support. For example, growing tensions in regions such as the Sahel and the Balkans could result in new conflicts with non-state combatants, which might prompt the UK to consider peacekeeping operations. Alternatively, growing tensions in the South China Sea or some kind of confrontation between China and Taiwan, ranging from a blockade to a full-scale invasion, may necessitate the UK considering lethal aid or economic sanctions, as has been the case with Russia's invasion of Ukraine.

Finally, increased tensions between nuclear powers and advances in emerging technologies are making a war involving weapons of mass destruction more likely. Russia has repeatedly threatened to use nuclear weapons over the war in Ukraine and has suspended its participation in the New START agreement on nuclear-arms reduction with the US. Furthermore, the US and China are in an arms race to develop lethal-autonomous-weapons systems, which will require careful handling to ensure they are used ethically. And advances in biotech also increase the risk of biological weapons being deployed by rogue states or terrorists.

05

A Changing Context Requires a Changed Approach to Strategy

This section sets out how government can adapt to develop the right strategy on national security, connecting everything from defence to diplomacy and development. This includes new structures at the heart of government to assess threats and ensure cross-departmental thinking, and new approaches to engagement with the private sector. The successful implementation of a reimagined national-security strategy rests on the processes that underpin its delivery.

SETTING STRATEGY FROM THE CENTRE OF GOVERNMENT

The starting point for a reimagined national-security strategy is ensuring that it is set by the centre of government and then delivered by the whole of government, and all the instruments of national power.

The New National Purpose papers published by the Tony Blair Institute for Global Change (TBI) have made clear the vital role the centre of government holds in bringing coherence and clarity and driving delivery and integration. It is critical that the teams working at the centre of government include genuine experts from industry who have the power to override traditional Whitehall controls, which is why we have repeatedly called for a science and tech policy and delivery unit that works across Number 10 and the Cabinet Office. This would ensure "the full weight of the prime minister's authority behind it and, at the core, the skill set to ensure its effective implementation".[8]

The success of a reimagined strategy for any issue of national importance, whether science and technology or national security, will depend not just on drive and delivery from the centre of government, but on reorganisation from within to make it happen.

DELIVERING THE STRATEGY REQUIRES A WHOLE-OF-GOVERNMENT APPROACH

The diverse range of threats facing countries requires a holistic response from government. The challenges cross departmental boundaries; so too must the

administrative response.

While the focal point of a new strategy will be the centre of government, its delivery will fall to the whole of government. This requires breaking down boundaries within government and establishing new structures to enable better cross-government working.

In the UK context, a key barrier is the relationship between the Foreign Office and the Ministry of Defence (MoD). The expanded role of the Foreign Office, which now encompasses international-development spending, makes a closer relationship with the MoD even more essential. It has been suggested by some that this integration should be further deepened by also moving trade policy within the Foreign Office, to facilitate even closer cooperation with the MoD and a truly holistic national-security policy, and this should be actively considered. A closer link between trade and foreign policy would help ensure that diplomatic efforts are coordinated, which in turn would strengthen commercial diplomacy and outreach as well as tech and commercial partnerships with allies. It would also allow the UK to take a more strategic approach to trade policy, prioritising issues such as deeper engagement with the increasingly important non-aligned countries.

Sustainable cross-departmental working and delivery should be underpinned by a new approach from the Treasury. A long-term defence-and-security strategy requires sustainable funding. In the UK, the Ministry of Defence is funded on a yearly basis, with a rolling budget, and the overall strategy is set by Number 10. This allows difficult budget decisions to be pushed down the road and is insufficient for a truly holistic national-security strategy that requires stable, consistent and long-term funding, and the delivery of complex capital programmes that require multi-year programme management.

The most critical element of a reimagined defence strategy is technology and the new capabilities it presents. This requires more cooperation between the Department for Science, Innovation and Technology and the centre of government. Deeper interaction on this area of policy should enable a rolling assessment of the tech capabilities needed for effective defence.

Breaking down all these barriers will require a new strategy and reporting structure from the centre of government that ensures all the moving parts – across departments, as well as outside government – can be galvanised swiftly and efficiently towards the same aim.

DRIVING STRATEGY AND DELIVERY FROM THE CENTRE OF GOVERNMENT

The prime minister requires the capability to set and drive defence strategy from Number 10, not just at the time of security reviews but on a rolling basis. Bringing greater expertise into the centre of government would make it easier for the prime minister to effectively drive change through the cross-departmental National Security Council. Achieving sufficient drive from the centre will require changing the structures at the heart of government.

Two reforms in particular would help to deliver this capability.

First, the creation of a **new National Security Team** in Downing Street. At present, central government expertise on security is provided by a team of about 200 civil servants, diplomats, and intelligence and military officers across the National Security Secretariat (NSS) and the Joint Intelligence Organisation in the Cabinet Office, and a senior civil servant with the title of national security adviser. While doing much good work, this team is too large, lacks focus and has limited expertise in areas of increasing importance to defence, such as advances in science and technology.

The centre of government needs a smaller, focused and more specialised National Security Team in Number 10. This team would set the defence and security strategy for the country, articulating the strategy's ends, ways and means over a two-, five- and ten-year horizon. This strategy would then be reviewed on an annual basis by a National Security Assessment. This annual refresh would allow the strategy to stay alive to shifting and new trends as well as new national-security risks.

This team would comprise individuals with a range of backgrounds and experience. This would include military and technology experts, strategists and procurement specialists, as well as representation from across government and the national-security community.

The team must be led by a politically appointed national security adviser who has the skills necessary to keep security policy at the heart of the government's political agenda. Alongside leading the National Security Team, their role would involve advising the prime minister and Cabinet on national security and engaging a network of the most senior international political, diplomatic, military and intelligence stakeholders, and experts from the defence and technology sectors.

The National Security Secretariat at the Cabinet Office would continue to be led by a senior civil servant, to support the work of the National Security Team and drive the implementation and delivery of national security policy across Whitehall.

Second, **a Centre for Strategic Futures should be created**. This team would report to the new National Security Team in Number 10 and its focus would be to assess trends and scenarios shaping key areas, such as technology, security and the economy, over a 20- to 30-year period. The Centre for Strategic Futures would feed into the National Security Team's security and strategy reviews.

On an ever-evolving global landscape, where the ripple effects of seemingly minor crises can escalate into significant global challenges, the centre would adopt a proactive approach to planning and strategic foresight. Early warning signals of major crises and conflicts often go unnoticed, resulting in a missed opportunity to avert them.

The centre would address this critical gap by enhancing the government's capability to assess the threat environment and anticipate potential risks (as well as opportunities) well in advance. While some government teams, such as the Defence Science and Technology Laboratory's Exploration Division,[9] already perform similar roles, to make a real difference to policy this expertise must be readily available at the heart of Number 10. The centre would not only focus on predicting possible crises in a holistic and interconnected manner, but also on providing the National Security Team with robust preventive strategies to avert such crises where possible. In instances where prevention is not possible, the centre would ensure that the government had options to prepare the most effective defensive and mitigation strategies.

A critical task for the National Security Team would not simply be to oversee the process of strategy development, but to shape it. This would require conducting a thorough and hard-headed assessment of threats and capabilities, taking into account the full spectrum of potential conflicts in the near- to mid-term, as outlined earlier in this paper. Holistic risk-based threat assessments and horizon scanning will be key to countering the challenges of the shifting geopolitical realities and hostile security environment that the UK will continue to face in the coming years.

ENGAGING WITH THE PRIVATE SECTOR EARLIER AND MORE EFFECTIVELY

A deeper, more strategic and ongoing relationship between the state and the private sector will be essential to delivering a reimagined national-security strategy. This is particularly true in terms of having the tech available for the conflicts of today, not just those of tomorrow.

This requires expanded engagement with the private sector from an earlier stage, allowing two-way discussions about the challenge, rather than following a model of procurement based too heavily on solutions conceived by government alone. This will allow more forward-looking and creative ideas to emerge, and different solutions to be brought to the table from the start.

Building formal and ongoing engagement mechanisms between the National Security Team, the Centre for Strategic Futures and the private sector would provide opportunities for fresh thinking from outside government to be built into decision-making inside government. These two governmental teams should hold monthly closed-door sessions with a range of expert representatives from the private sector. These would involve scenario mapping, wargaming, threat assessments and capability reviews.

These ongoing interactions would feed into the direct work of the National Security Team, the Centre for Strategic Futures and government procurement processes.

SOFT-POWER CAPABILITIES

The future of defence will require military capability to be fitted into a wider set of capabilities. The ultimate aim of having the right security strategy is to avoid war through deterrence. To achieve this, further tools are needed beyond traditional military strength.

The right defence posture necessitates a new approach to foreign policy. Diplomatic networks and methods today are largely shaped by the habits of the past, not the capabilities of the future. The set-up of embassies, the work of diplomatic staff and the tools used to work through diplomatic strategy are largely outdated. Avoiding war, navigating war and ending war all require diplomacy. So states should examine, as part of their reimagining of defence and security strategy, their diplomatic reach and capability. Fully harnessing the possibilities of technology will be a key part of this, alongside other forms

of soft power, including the creative industries.

Traditionally, international security and diplomacy were primarily the domain of foreign ministers, senior diplomats, defence ministers and senior military officers. But tech is now a major part of foreign policy, from malicious non-state actors to big tech companies. AI and other emerging technologies are fundamentally altering the nature of international relations and diplomacy, and are central to the great-power competition between the US and China.

In 2022, TBI published *A Leaders' Guide to Building Tech-Forward Foreign Policy*, demonstrating the need for countries to build tech into their foreign-policy strategies for greater situational awareness, coordinated vision and strategic policy positions. From tech and cyber ambassadors to education on new tech in foreign-service academies, integrating tech and diplomacy will be a key tool in helping states to advance their reach and capabilities.

Emerging technology also has the potential to improve a variety of diplomatic capabilities, including information gathering and analysis, translation, negotiation and detection.

A further dimension is aid policy. The right security and defence policy will take every viable step to use diplomatic and soft-power capabilities to avoid conflict. Putting the right development policy in place is a key part of this. The fact that the UK's international-development department now sits within the Foreign Office allows the country to make sure that this area of government policy is given strategic direction to align with national-security considerations. This will ensure that spending is aligned with preventing conflict and offsetting potential risks, like climate change, and stabilising areas already in or recovering from conflict.

The National Security Team should include representation from the international-development department within the Foreign, Commonwealth & Development Office. This interaction, with wider oversight from the National Security Council and prime minister, will guarantee that the government's defence and security strategy is fully aligned with overseas-development spending and policy. Crucially, these strategies must carefully align with, and be augmented by, those of the UK's allies and the international organisations of which it is a member.

RECOMMENDATIONS IN REVIEW: STRATEGY

- **Create a new National Security Team** to reflect the importance of delivering a reimagined defence and security strategy that secures the country against a new era of threats. This team would be enhanced both in its role and the type of personnel it recruits. It would give Number 10 the central capability to set, drive and continually evaluate the country's defence and security strategy.
- **Establish a Centre for Strategic Futures** as part of a new architecture to think through future defence challenges as well as current ones. This would sit outside government structures but report into the National Security Team; its key role would be to assess future threats beyond the horizon of National Security Assessments. It would comprise recruits with a variety of backgrounds to bring long-term but radical thinking, including scientists, tech and defence experts, diplomats and climate experts.
- **Create a sustainable funding model for defence and security**. An effective and sustainable national-security strategy requires consistent funding across a clear timeline, to allow the right investment and long-term thinking. Working with the prime minister and the National Security Team, a multi-year budget framework should be agreed for defence in order to provide the clear funding path needed. This budget would be reviewed by the National Security Team, working closely with the Treasury, to ensure that new threats can be tackled, and capabilities and opportunities can be seized.
- **Set up new engagement mechanisms between the private and public sectors**. For too long, the state has interacted with the private sector in a way that serves neither well. This too often results in final tenders for capabilities being issued without prior consultation with the defence industry and external experts; closer and earlier engagement is required. To address this gap, monthly closed-door sessions should be held between the National Security Team in Number 10 and private-sector companies and representatives. These sessions would include horizon scanning, scenario planning and wargaming. This closer collaboration will allow the private sector to be engaged in thinking through the defence problems that the country faces, not just be presented with solutions shaped only by government. The strategic advantages group set up in Number 10 (under John Bew) made important strides in establishing this work, but it must be widened and deepened.
- **Refresh soft-power capabilities**. The UK's defence and security

capabilities are not confined simply to the military, but include important soft-power levers – diplomacy and development policy, in particular. The National Security Team would align defence policy more closely with diplomacy and aid spending, while making sure that both of these areas fit carefully into the capabilities of the UK's allies and alliances.

06

Curating Agile and Adaptable Integrated Capabilities

New technologies have always changed the character of warfare and the conduct of wars, but neither technological advantage nor boots on the ground alone can win today's conflicts. Instead, advantage is gained by those who can integrate new technologies most swiftly and seamlessly into their capabilities, operating concept and actions. Technology has shifted the balance of power in favour of those who can use lightweight but heavy-impact tools, from swarms of bots exacerbating societal divisions and controlling narratives to home-made drones targeting global shipping, leading to a new economics of warfare. As such, traditional heavyweight capabilities and expensively crewed platforms lose both their cost effectiveness and deterrent effect when trying to counter coordinated cross-domain attacks involving increasingly smaller capabilities that can swamp defences. Distinctions between foreign and domestic defence are blurred as hybrid warfare places critical national infrastructure, supply chains and the communications networks on which the UK economy depends on the "front line".

The future of warfare is no longer a choice between boots on the ground and technological prowess – it is the intelligent fusion of the two across all domains. This requires moving beyond the concept of "joint" operations to the integration of a broad range of technologies at speed and scale, both backstage and in the theatre of war, to bolster societal resilience and deterrence. From integrating AI-enabled processes to establish smarter procurement from the factory to the battlefield, to harnessing those that can build information advantage, a new vision for capabilities needs to be adopted.

To deter and defend today, as well as prepare for the future of multi-domain warfare, the UK government needs to take a five-pronged approach.

First, **secure and accelerate critical current capabilities**, from ensuring the resilience of the UK's most large-scale capability to the deployment of more agile capabilities at speed.

Second, **identify and procure key near-term needs and capabilities** that can be integrated to meet the challenges of near-term conflicts.

Third, **envision and prepare new longer-term cutting-edge capabilities**, drawing on future scenarios and key relationships with industry to accelerate the absorption of critical technologies that can engage and constrain across all domains.

Fourth, **review, repurpose, retrain or retire** any capabilities that cannot be easily adapted to function effectively in the new integrated-warfare vision, to free up investment in new capabilities.

Fifth, **maintain leadership on the international stage to consolidate influence** in shaping international frameworks and the governance of future military capabilities.

SECURING CURRENT MULTI-DOMAIN CAPABILITIES

An integrated approach to operational capability relies on three key elements: **protect, engage and constrain**. This requires a foundation that can deter and deny, which means bolstering the UK's most powerful capabilities to maintain their readiness and resilience.

Ensuring the continued effectiveness of the UK's **nuclear-deterrent capability is an urgent priority**. Earlier this year the test firing of a Trident missile from a Royal Navy submarine failed, following a similar test failure in 2016. The MoD states that this test is not cause for concern, but the Royal United Services Institute (RUSI) has warned that from the outside it is impossible to gauge how significant the test failure was.[10] It is potentially notable that US tests using the same missiles have been successful.

This has raised questions about the UK's ability to deploy nuclear weapons. As the nuclear deterrent only works if foreign adversaries know that the UK's weapons can be deployed, the next government must be sure that the deterrent threat is credible.

Next, maintaining the UK's **subsea capabilities** is also critical to ensuring its protection. The UK's anti-submarine warfare capabilities are an important aspect of European defence, with many other NATO countries lacking these capabilities. With the UK specialising in this area already, expanding support would benefit NATO. Furthermore, given Russia's use of mines to attack civilian

shipping in the Black Sea, the UK should expand its maritime minesweeping capabilities to help respond to a Russian attack on NATO.

As the information domain is increasingly crucial for constraining adversaries' erosion of societal resilience, the UK must also urgently bolster its approach to **countering information warfare and conducting influence operations**. With China and Iran joining Russia as key players in the information domain, the UK needs a better strategic narrative to deter, deny and counter disinformation campaigns at home and abroad.

In the short term this includes boosting key levers of soft power and influence such as the **BBC World Service.** The BBC plays a crucial role in bringing impartial news coverage to countries where the Kremlin and other autocracies are seeking to foment social unrest or hatred of the West. For example, the latest figures show the BBC World Service has an average weekly reach of 19.2 million for its Persian-language service, 5.6 million in Russian and 700,000 in Serbian.[11] In recent years the BBC has cut 400 World Service jobs due to the need to save £30 million per year on its international services, and Director-General Tim Davie has warned that its revenues are currently insufficient to fund both domestic and international services.[12] **The government should therefore increase its direct grant to the BBC World Service at the next spending review**.

Simultaneously, the UK needs to explore longer-term reinforcement of a more cohesive **national influencing directorate or information agency** to promote British narratives. As former Commander of the US Office of Naval Intelligence Mike Studeman has argued, Western information operations are often too subdued.[13] Greater training of information professionals cutting across different government departments with more unified approaches to building information resilience is key to countering information warfare at pace.

IDENTIFYING AND PROCURING NEAR-TERM NEEDS AND CAPABILITIES

The evolution of the war in Ukraine and the escalation of conflict in the Middle East have highlighted several key areas of near-term needs and capabilities that must be urgently addressed in order to actively defend, deter and deny at scale and pace. This includes identifying gaps in the regional and national defence architecture, establishing a supply of short-term capabilities such as drones, and bolstering the cyber and cyber-physical communications infrastructure on which UK capabilities rely.

Addressing Gaps in European Defence Architecture

The most urgent defence priority for the next government is working with European allies to identify and jointly procure capabilities where NATO is over-reliant on the US, in order to defend Europe from Russia in the event of reduced US support.

First, the UK and Europe need to urgently invest in stronger **integrated air and missile defence capabilities ahead of any Russian attack on NATO.** NATO officials have calculated that the alliance currently has fewer than 5 per cent of the air defence capacities necessary to protect central and eastern Europe against a full-scale attack.[14] Northrop Grumman UK has warned that the UK's air defence capabilities are "very limited, to the point of being negligible" due to "long-term under-investment and an over-reliance on NATO partners' capabilities".[15] The recent Iranian missile attack on Israel, as it also combats missile attacks from Gaza, Lebanon and Yemen, highlights the need for defensive systems such as the Iron Dome and David's Sling to detect and intercept these threats at pace and scale. To counter this, RUSI has called for the UK to develop a command-and-control architecture that "controls an appropriate mix of sensors and effectors", so that air defence capabilities can detect and intercept missiles at speed.[16]

Another critical capability to urgently secure is the ability to destroy enemy air defences. Professor Justin Bronk of RUSI has warned that NATO is "heavily dependent on the US" for "the ability to roll back Russian ground-based air defences from the air". He states that NATO's ability to defend Europe is based on achieving air superiority and that reduced US support in this area would damage security. Therefore, Europe must "rapidly procure specialised weapons and dedicate serious aircrew training time and focus to developing high-end suppression and destruction of enemy air defences (SEAD/DEAD) capabilities".[17] As part of this, the procurement of SPEAR 3 missiles should be explored. RUSI has also warned that Europe lacks its own long-range strike capabilities beyond the 300 km range, and that so far efforts to plug these capability gaps are "scattered and certainly not enough".[18] **Alongside a full review of European capabilities, the next government should take urgent and immediate action to plug these SEAD/DEAD and long-range missile capability gaps.**

Adapting to a New Era of Drone Warfare

Drone warfare has become a key characteristic of recent warfare, from Nagorno-Karabakh to Ukraine and more recently in the Red Sea. This builds on similar dynamics to those used by the Islamic State, which launched 60 to 100 drone attacks per month across Syria and northern Iraq in 2017,[19] and is altering the symmetry, pace and economics of conflicts.

Drones have been critical to conducting strikes on enemy forces, notably attacks by Ukrainian forces on Russia's Black Sea fleet using underwater drones, and for targeting artillery strikes, helping to save munitions.[20] But they are key to supporting surveillance and intelligence gathering too, allowing the collection of data on enemy bases and troop movements. The photographs and videos obtained by drones are also being used to capture international attention.

The pace at which drones are being deployed – Ukraine is losing 10,000 a month – demonstrates that Western countries will need to be able to mass produce cheap drones at a rate that can allow lost ones to be easily replaced, as well as increase opportunities to train operators.[21] Russia has indicated that it will start programmes in schools to teach young people to produce and operate drones to meet this need. The US has instituted its Replicator programme, which is designed to mass produce cheap drones.

However, the drones in current use are well suited to current conflicts that involve dense forces in close proximity, often in urban or semi-urban environments. Their effectiveness is not yet proven in more open or extreme environments such as jungles or the Arctic. New investment will be needed for capabilities that can operate across environments.

As they develop, drones will be deployed for a multitude of uses, including monitoring and deterring attacks on undersea cables and supporting counter-terrorism operations. Western countries will need a balance of both cheap, mass-produced drones and expensive, highly specialised ones to cover different uses. Threats will increase as a result of drones of different sizes being combined in new ways that allow for constraints to be overcome, and as more intelligent micro-drones emerge that could be almost undetectable to the naked eye.

For a country such as the UK with a sizeable navy, underwater drones will be

especially important for protecting vulnerable vessels such as aircraft carriers and strategically critical vessels such as Trident submarines. At the same time, new counter-drone technologies are being developed that will reshape their effectiveness. Therefore, procuring drones and the software to use them, and investing in counter-drone technology, are both critical to the UK's near-term and longer-term defence.

New players, such as US defence-technology company Anduril, are leading in developing collaborative combat aircraft (CCA). These lay the foundation for the use of swarms of uncrewed systems and unmanned "wingmen", to allow pilots to return unharmed, highlighting the new frontiers of unmanned capabilities. Maintaining a sharper focus on developing drones strategically will be key, bearing in mind that not all drones are equal: some are highly specialised and expensive, while others will be cheap and disposable. This requires a more holistic approach to the drone ecosystem, to move beyond the current needs of disposable drones in one particular conflict.

The UK's £4.5 billion Defence Drone Strategy is a step in the right direction, with its focus on building a stronger industrial base and securing faster acquisition, but more fundamental reforms to defence procurement will be needed if the strategy is to be a success.[22]

Harnessing Cutting-Edge Software

AI systems are a critical capability for all four of the scenarios described earlier in this paper for which the UK needs to prepare. They underpin the capabilities of hardware such as drones, as well as being essential for command-and-control systems. This is an area in which the West, as the home of companies with advanced defence AI capabilities such as Anduril, Palantir and Helsing, holds a distinct advantage over Russia. Microsoft is already working to deliver a prototype edge-compute platform to support the Royal Navy by promoting the interoperability of different combat systems.[23] The main barrier to making full use of these advantages in the UK is that the country's defence-procurement system is not well suited to securing software from startups and remains focused on securing hardware from well-established vendors. Our proposed reforms to defence procurement are set out in the next section.

Strengthening Cyber Capabilities

As the technologies utilised in both daily life and defence become increasingly interconnected, threat vulnerabilities expand. The hybrid-warfare approach of countries such as Russia, that incorporates cyber and information warfare into conventional military action, requires an integrated defence across the cyber domain as a whole.

While the war in Ukraine has been dominated by land activity, **cyber and electronic warfare have become critical capabilities in supporting conventional military activity.** Cyber operations to disrupt and degrade systems – such as the Russian cyber-attack targeting Ukraine's power infrastructure with Industroyer2, a new variant of the malware used to attack its power grid in 2016[24] – are a key tool of warfare. Similarly, control of the electro-magnetic spectrum is critical to impacting the effectiveness of precision-guided munitions, as well as confusing air defences.[25]

The nature of current warfare has pushed Ukraine's allies to strengthen their cyber shields as they find themselves targeted by state-linked cyber actors, as well as geopolitical hacktivists with their waves of distributed denial of service (DDoS) attacks. In the first six months of the Russia-Ukraine war, the share of global cyber-attacks impacting EU countries increased from 10 per cent to 46 per cent. Russia's Sandworm hackers were linked to a significant attack on Danish energy infrastructure in 2023.[26]

At the same time, **Beijing's advanced cyber capabilities are being leveraged to access critical infrastructure and steal Western intellectual property.** Earlier this year it was revealed that Chinese hacker group Advanced Persistent Threat Group 31 (APT31) had targeted thousands of Western politicians, foreign-policy experts and others as part of Beijing's foreign-intelligence and economic-espionage objectives.[27] Further, US intelligence agencies revealed that the Chinese Volt Typhoon group had been active in critical infrastructure networks for half a decade, pre-positioning for an opportunity to cause major disruption.[28]

Other rogue states, terrorist groups and malicious actors are developing stronger cyber capabilities, as well as utilising networks of ideologically motivated hacktivists. North Korea has hacked the emails of South Korean officials, stolen $3 billion and tried to access semiconductor technology.[29] Iran has deployed cyber-attacks on US water plants and TV streaming services in

the UK, the UAE and Canada,[30] and rapidly increased the pace and scale of its operations through surging support to Hamas in the Hamas-Israel war.[31] With the advent of generative AI tools, malicious actors and violent extremists are now able to accelerate their activities,[32] making the need to "defend forward" to prevent malicious cyber activity all the more urgent.

The UK needs to continue to **prioritise the procurement of advanced cyber capabilities** and the **recruitment and retention of personnel skilled in cyber operations** to help support the National Cyber Force and National Cyber Security Centre to defend forward across critical national infrastructure.

Strengthening Communications Resilience: From Subsea Cables to Satellite Communications

Current and emerging networked capabilities rely on a massive global network of undersea cables and satellite infrastructure that is increasingly susceptible to attack. The MoD reports that 99 per cent of global internet traffic passes through undersea cables, while gas and oil pipelines and electricity interconnectors are critical in terms of the UK's energy trading with Europe.[33] NATO officials have warned that Russia is actively mapping allied seabed infrastructure and that "there are heightened concerns that Russia may target undersea cables and other critical infrastructure in an effort to disrupt Western life".[34] Meanwhile, US experts have suggested that Huawei's involvement in many undersea cables might enable "China to attach devices that divert or monitor data traffic – or, in a conflict, to sever links to entire nations".[35]

Recent incidents involving undersea infrastructure have highlighted growing concerns about its vulnerability. A recent report by UK-based think-tank Policy Exchange found that since 2021 there have been eight unattributed-yet-suspicious cable-cutting incidents in the Euro-Atlantic and more than 70 publicised sightings of Russian vessels behaving abnormally near critical maritime infrastructure.[36] In 2023, Chinese vessels severed cables in the East China Sea, either by accident or by design, impacting Taiwan.[37] Houthi attacks in the Red Sea indirectly damaged undersea cables earlier this year, with a damaged ship affecting 25 per cent of data traffic between Asia and Europe.[38]

Seabed infrastructure is equally at risk from environmental events and even accidents as a result of commercial maritime activity. Damage to three cables

off the coast of West Africa that led to widespread outages was likely caused by a seabed rockslide[39] and the five-week outage on the island of Tonga was the result of a cable severed during a volcanic eruption.[40] With limited entities able to repair these cables, urgent action is needed to both tighten the international governance regime of the cable infrastructure[41] and strengthen rapid-repair forces.

Allied forces are now conducting more underwater exercises involving seabed infrastructure surveillance, including through AUKUS and the Joint Expeditionary Force,[42] and NATO is establishing a Maritime Centre for the Security of Critical Undersea Infrastructure within the UK, as well as a Digital Ocean initiative to coordinate national and allied capabilities employed for maritime surveillance, from satellites to underwater drones.[43] New capabilities are being developed that allow the cables themselves to act as sensors to threats, as a new forward-looking solution for resilience.

While the UK has recently purchased two Multi-Role Ocean Surveillance ships to monitor critical seabed infrastructure, they are unlikely to prove sufficient on their own.[44] **The National Security Team should consider investing more in surveillance of undersea infrastructure to reduce the risk of an attack and develop a clear plan for rapid incident response and remediation.**

Current and emerging defence capabilities, as well as the systems underpinning daily life and consequently national resilience, are **reliant on satellite data and communications**. Ensuring the resilience of this architecture as well as viable alternatives is critical for deterrence.

The importance of satellite systems for warfare has been highlighted in Ukraine, with Starlink satellites allowing Kyiv to maintain internet and communications networks. This has proved critical for both civilian and military purposes, made the use of drones and autonomous systems more possible and significantly strengthened Ukraine's war efforts.[45] While the West may have some advantage now, with more than half of the active satellites orbiting the Earth belonging to NATO members or companies based in their territories,[46] the constellations remain at risk of space debris, the Kessler syndrome problem, space weather events and anti-satellite weapons.

Recent reports say that Moscow is developing an anti-satellite nuclear weapon, in contravention of the Outer Space Treaty,[47] that would be capable of attacking groups of satellites through an immediate electromagnetic pulse

and longer-term radiation decay, to which "unshielded military and almost all non-shielded commercial satellites would be potentially vulnerable".[48] Both Russia and China have already developed missiles capable of destroying individual satellites in low-Earth orbit which, if deployed in sufficient numbers, would also create enough debris to render parts of space unusable.

Alongside these missiles, **both countries are finessing other capabilities for damaging Western satellites**. For example, China's Shijian-17 satellite has robotic arms designed for satellite repair but also capable of grappling and damaging other satellites.

Risks are increasing as lower costs and new alliances allow rogue actors to project power in space. North Korea recently launched a spy satellite into orbit and announced plans to launch a further three this year.[49] Iran is also increasing its space presence, with Russia having launched the Pars 1 Iranian satellite in February.[50] The UK's Space Directorate has warned that the falling cost of access to space could increase the potential for terrorist attacks on objects in space.[51]

Global Positioning System (GPS) interference remains a pervasive problem, impacting the resilience of satellite communications. Both Russia and China have developed ground-based lasers capable of blinding satellite sensors, as well as jammers to disrupt satellite communications.[52] Recent disruptions to GPS around the Baltic have been attributed to Russian interference using low-cost jamming techniques,[53] while Israel has engaged in defensive jamming to pre-emptively prevent incoming drone and missile attacks from Iran and Hezbollah.

The challenge of first-mover advantage in the space domain is that the Western constellations are old and lack the stronger anti-jamming defence of, for example, China's BeiDou system.[54] Many Western satellites launched in the late 1990s are still operational even though they were only intended to have a seven-and-a-half-year life span. These are based on L1 frequency, which is easy to jam, have limited security and lack anti-jamming techniques. More resilient solutions for beyond-line-of-sight communications and navigation systems are urgently needed.

In the medium term, the National Security Team must invest in more resilient and diversified space systems. This includes upgrading to more modern and secure signals, such as L5 frequency, to address jamming issues,

and working towards more operationally responsive space capability through which the UK can rapidly augment capabilities or replace lost ones. Working towards more diversified capabilities, such as satellites in low-Earth orbit, can reduce the impact of an attack on traditional satellite systems in medium-Earth orbit. The UK also maintains a stake in Eutelsat OneWeb, which is seeking to launch a network of second-generation OneWeb satellites and is talking to export-credit agencies, including UK Export Finance, to raise the necessary funding.[55] Similarly, high-altitude platform stations can also offer many of the same functions as satellites, with AALTO HAPS' Zephyr[56] and BAE Systems' PHASA-35 expected to enter full commercial service in the next couple of years.

Protecting Biosecurity

Finally, biosecurity capabilities will also be a critical capability for the UK to develop. As outlined in our previous report, *A New National Purpose: Leading the Biotech Revolution*, advances in AI and biotech mean that sophisticated bioengineering capabilities will become increasingly accessible to rogue states and terrorist organisations over the next decade.[57] The capability to rapidly design and manufacture vaccines at scale will become increasingly important to Western defence and security. Global monitoring capabilities to detect new viruses quickly will also be important, with biotech companies such as Ginkgo Biosecurity Services seeking to establish these capabilities.[58]

PREDICT AND PREPARE NEW LONG-TERM CAPABILITIES

Alongside near-term priorities, the UK will also need to prepare to procure longer-term capabilities to defend itself in the 2030s and beyond. The MoD's 2021 Integrated Operating Concept sets out priorities that include securing smaller and faster capabilities that can avoid detection, capabilities to respond to electronic warfare and make use of more sophisticated networks of systems, an increased focus on stealth capabilities, and a mix of crewed and autonomous platforms.[59]

Given these priorities, there are three pivotal capabilities that are central to securing the UK's defence from the 2030s onwards.

First, continued support is needed to build next-generation stealth fighters. Significant funding has already been invested in the UK's Global Combat Air Programme with Japan and Italy, through which the three

countries will develop a new sixth-generation combat aircraft, Tempest, to come online in 2035.[60] To date, the government has invested about £2 billion in this programme, with another £10 billion to £15 billion expected over the next decade.[61]

Second, greater investment is required in the development of the next generation of uncrewed and autonomous capabilities. Drones have become a critical part of current capabilities in this area, but countries are already procuring new forms of uncrewed hardware for human-machine teaming. For example, Anduril is producing an unmanned submarine for Australia – the Ghost Shark – which can dive deeper than conventional submarines, a critical capability for maintaining the ability to avoid detection as objects in oceans become more easily detected.[62] Meanwhile, the US is exploring the use of ground robots that can be deployed in human-machine teams, with the potential to reduce human casualties in combat. [63]

Third, long-term support for the UK's quantum ecosystem and its application to defence is required. Once it comes on line, quantum machine learning will revolutionise processes with an impact far greater than that of generative AI. New quantum position, navigation and timing (PNT) technologies – already trialled for commercial UK flights[64] – and quantum communication technologies, would help mitigate the impact of the kind of attacks on satellites discussed earlier. Quantum sensors would help the UK armed forces find targets of interest and enhance situational awareness. Quantum computing would help spot patterns and break encryptions, as well as unlocking more powerful AI for defence applications.[65]

As such, quantum-resistant security needs to be developed and baked into new capabilities simultaneously, and steps taken to counter action that could be taken on quantum analysis of data already in the hands of adversaries. Establishing leadership in the development of military quantum applications will require new allied partnerships with the likes of Japan,[66] alongside existing partnerships such as AUKUS Pillar 2.[67]

REVIEW, REPURPOSE, RETRAIN OR RETIRE CAPABILITIES

As the nature of defence and deterrence evolves, so must the arsenal of capabilities. As resources and funding will always be limited, **choices may need to be made as to which capabilities should be deprioritised** if they cannot be repurposed. Advances in technology will accelerate the need for

focus and prioritisation, with emerging technology rendering more existing capabilities redundant over time. Identifying and reducing support for these capabilities will be key.

Furthermore, rather than trying to maintain every defence capability and often doing so insufficiently well, the UK must focus on delivering key capabilities effectively. Alongside this, it should specialise in capabilities where it is well equipped to do so and can offer significant advantage to collective defence partnerships, such as NATO. This will require hard-headed prioritisation across all the services.

There is evidence to suggest that neither the government nor the armed forces are currently taking these kinds of decisions. Earlier this year, the Public Accounts Committee found a £16.9 billion deficit between the MoD's stated capability requirements and its budget, warning that "the MoD has not had the discipline to balance its budget by making the difficult choices about which operational activities to curtail and which equipment programmes it can and cannot afford".[68] Similarly, experts have warned of cultural barriers to this kind of prioritisation within the armed forces, with some senior leaders concerned that winding down certain capabilities jeopardises the perception of our armed forces as a tier-one fighting power.

Keeping the UK safe means ensuring that **credible core capabilities are top-tier and readily available**. Much of the uplift in defence spending proposed by the current leadership will be used to meet previous commitments, and while there is considerable public support for higher defence spending, voters are evenly split on whether such a policy would actually make the UK a safer place to live.[69] **The next government will need to be clear on both how additional defence spending makes the country safer and how it delivers value for money by deterring adversaries** from starting costly wars.

Identifying the capabilities that need to be repurposed, retrained or retired will need to be informed by a **comprehensive, uncompromising and forward-looking strategic review** that incorporates a broad spectrum of thought and expertise. This will judge current capabilities not just by the benchmark of today's wars and operating environments but by all the future environments to which the UK may have to adapt. The National Security Team may consider whether more manoeuvrable divisions with counter-drone technology rather than heavy-armour capabilities would better support NATO defence, given that many European countries have stronger heavy-armour capabilities.

Consideration could be given to the extent to which drones could meet some of the UK's defence needs better than legacy crewed aircraft. How far redeploying manpower from the Royal Navy's aircraft carriers to other naval capabilities would improve the UK's defence should also be considered, given the personnel challenges in this service.

LEADING GLOBAL GOVERNANCE FOR LONG-TERM INFLUENCE

More powerful capabilities will also require robust multinational frameworks for governing their responsible use. The international architecture for governing powerful technologies largely dates from the Cold War, and risks being rendered obsolete by military advances in areas such as AI, biotech, space and cyber. The National Security Team must explore what minimum international guardrails are needed to create significant geopolitical consequences for irresponsible use and maximum deterrence, as well as ensuring the sustainability and resilience of key architecture on which UK capabilities rely.

The UK has already played an important role in shaping governance of **military activity in space**, successfully pushing for an Open-Ended Working Group (OEWG) at the UN. But while the OEWG made useful recommendations, including norms on refraining from deliberate damage to satellites, no procedural progress was made due to Russian intransigence.[70] The UK also plays a strong role in the UN Committee on the Peaceful Uses of Outer Space and in funding a number of initiatives through the UN Office for Outer Space Affairs to promote **long-term sustainability guidelines for space and wider capacity building on space regulation**. Future areas to explore include the establishment of an International Space Safety Organisation to inspect and enforce internationally agreed regulations. [71]

There is currently no effective regime to hold saboteurs to account for attacks on undersea infrastructure in international waters. At present, under the UN Convention on the Law of the Sea, the right to determine punishment of the perpetrator rests with the state whose citizenship they hold or under which the vessel operates.[72] The UK should work to help build a new set of regulations designed to **deter action on cables and hold perpetrators accountable** in the country of the cable owner.

The UK has already established itself as a key voice in establishing **global norms around ethical use of autonomous weapons systems.** Complexity

and challenges around agreed definitions have slowed the progress of the UN Group of Governmental Experts who have been considering the issue under the Convention on Certain Conventional Weapons since 2016, with very little beyond a set of 11 guiding principles having been agreed.[73] But the UK has led through its commitments set out in its 2022 Ambitious, Safe and Responsible Approach and its Annex C, dedicated to lethal autonomous weapons systems (LAWS). The UK has also played a key role at the Responsible AI in the Military Domain (REAIM) Summit and is a signatory to the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. The UK should build on its success with the AI Safety Summit and establishment of the AI Safety Institute to expand the frameworks for testing and evaluating AI in high-risk military AI systems and develop norms for applying existing international humanitarian law to the use of LAWS.[74]

The use of offensive cyber-security capabilities is another area in which norms need building. In 2023 the UN secretary-general called for an agreement that "infrastructure essential for public services and to the functioning of society is off-limits to malicious cyberactivity", backed by "an independent multilateral accountability mechanism".[75] This is the right long-term ambition.

Finally, international frameworks and capabilities on biosecurity are areas that the National Security Team must explore. As set out in previous TBI reports, the government should introduce rigorous DNA-synthesis-screening requirements in the UK and promote the adoption of these requirements across the wider international community

FIGURE 5

Key capabilities to defend today and prepare for the future of multi-domain warfare

Secure and accelerate	**Identify and procure (near term)**	**Predict and prepare (long term)**	**Review, repurpose or retire**	**International leadership for influence**
Trident as an active, independent capability	Integrated air-missile defence	Agile, adaptable and interchangeable capacities	Tackle cultural barriers resistant to capabilities review and reassessment	Strengthen guardrails around use of weapons in outer space
Funding for BBC World Service	Improved SEAD/DEAD capabilities and long-range strike capability	Next-generation fighters		Protections for subsea infrastructure
National Influencing Directorate	Sophisticated multi-level drone programme	Next-generation autonomous capabilities		International guardrails for use of AI in the military
	Stress testing critical national infrastructure for cyber threats	Quantum-safe and quantum-enabled defence		
	Diversified, jamming-resistant satellite system			
	Surveillance and protection of subsea infrastructure			

Source: TBI

RECOMMENDATIONS IN REVIEW: CAPABILITIES

- Ensure the UK's nuclear deterrent remains effective by conducting an urgent internal review. This should consider whether the UK's Trident programme has the British technical expertise and support to maintain the Continuous At-Sea Deterrent and fire missiles with or without the agreement of Washington. If capability gaps are found, take action to plug these gaps as soon as possible. Demonstrate Trident remains effective by conducting a successful test as quickly as possible.
- Increase funding for the BBC World Service to combat disinformation in priority countries and regions, such as Russia, the Balkans and the Middle East.
- Create a UK Information Agency, staffed by trained information professionals, to promote Western narratives and rebut adversaries' propaganda. Empower the agency to use strategic disclosure of intelligence to achieve this objective.
- Work with allies in Europe to plug high-risk capability gaps that would result from diminished US support, including SEAD/DEAD capabilities and long-range strike capabilities beyond the 300 km range, as a matter of urgency.
- Focus on the mass production of cheap, easily replaceable drones to support British surveillance, propaganda and strike capabilities.
- Develop integrated air and missile defence capabilities, with a focus on the command-and-control architecture controlling sensors and effectors, to allow the country's air defence capabilities to detect and intercept missiles at speed.
- Create a new AI red-teaming group to continually stress-test cyber vulnerabilities and critical infrastructure. If necessary, pull in expertise in this area from the National Cyber Security Centre, the AI Safety Institute and industry.
- Invest in procuring more resilient satellite capabilities. One way to do this would be to support Eutelsat in launching a network of second-generation OneWeb satellites.
- Work with allies to commission Western space companies to provide ongoing surveillance around critical seabed infrastructure, and to procure a greater number of underwater-surveillance drones.
- Reduce the cost of the Global Combat Air Programme to the UK by seeking to bring in other partners, such as Saudi Arabia.
- Increase funding for the military applications of the National Quantum Strategy, including PNT, at the next spending review. Work to ensure that

Japan can participate in the quantum aspects of AUKUS Pillar 2.

- Tackle cultural barriers to deprioritising capabilities that are not integral to the defence of the UK and its allies.
- Continue to push for international guardrails around responsible capability use to prevent military activities in space, attacks on undersea infrastructure, the development and deployment of LAWS in ways inconsistent with international humanitarian law, cyber-attacks on critical infrastructure and the use of bioengineering tools as a weapon of war.

07

Emerging Capabilities Require New Procurement Processes

Current models of defence procurement are costly, slow and lack sufficient innovation; they are not fit for purpose in today's dynamic and technology-driven threat landscape. This section sets out a clear roadmap for reforming procurement.

The ability to procure and produce at speed, scale and cost is essential for maintaining defence readiness. However, the current UK defence-procurement system lacks the dynamism and speed to effectively address the new threat landscape. In fact, the current system reflects the legacy of a bygone era: it is highly consolidated and overly bureaucratic; it is biased towards procuring large, complex hardware systems, as opposed to software systems and capabilities; and it has an institutional bias towards working with large, well-established "prime" defence contractors at the expense of innovative early-stage startups and small and medium-sized enterprises (SMEs).

The confluence of these dynamics demands, first and foremost, a rethink by the MoD on how it partners with industry and cultivates a co-design, co-build environment with the UK's top innovators. There has been limited progress in this area through the MoD's new Integrated Procurement Model, which commits to engaging the industrial base earlier to work on force and capability development, as well as delivering more transparency about the MoD's acquisition pipeline to help focus defence R&D efforts.[76] However, these changes are insufficient in terms of the scale of reform needed for procuring emerging defence capabilities.

On a strategic level, to meet today's demands the UK needs to undergo a paradigm shift in the types of weapons and weapons systems it procures. This requires a move away from large complex systems towards small, networked, low-cost expendable systems – at least where possible. To enable this shift, the UK needs to invest in a dedicated career path for a new class of procurement professionals specially trained in purchasing these new systems. This change also requires deeper coordination and alignment with key

defence partners (particularly the US) on the likes of people, funding and technology. AUKUS should provide the basis for a new method of joint development and capabilities.[77]

In this vein, the UK should avoid duplicating existing systems or capabilities within the alliance and instead invest in capabilities to augment them. The UK is in a unique position to lead with a specialisation on innovative defence technologies and capabilities, including efforts to boost mass production of low-cost defence systems.

Key reforms are needed to support MoD procurement and its ability to foster, facilitate and procure new technologies – and to transition these tools, quickly and at scale, into the hands of those who fight wars. This is central to the ministry's ability to stay ahead of this ever-evolving threat landscape, both now and in the future.

THE ON-RAMP

Fostering a diverse and vibrant defence base will serve as the cornerstone of an agile, innovative and resilient defence sector. A diversified and competitive market is essential for driving innovation and introducing new ways of thinking. Yet this is not always the case in the current defence sector: many experts question whether the highly consolidated defence industrial base can remain dynamic and respond to evolving hybrid threats. The MoD can counter this trend by prioritising investments in partnerships with private-sector innovators, including software companies and non-traditional contractors.

However, the same prime contractors are winning the majority of large defence contracts – and the model is both intentionally and unintentionally biased toward these companies. This is driven by a variety of factors. The very nature of the MoD's focus on hardware and big, complex weapons systems inherently favours many of the incumbent contractors. But even in the dual-use and defence-innovation ecosystems, experts say the complexity of procurement processes poses insurmountable barriers for smaller companies. That is because these companies do not have in-house procurement teams solely focused on identifying solicitations, navigating contract terms and red tape, nor managing relationships with the buyer.

Today's consolidated ecosystem shoulders out small innovators and

creates little incentive for the big contractors to innovate, take risks or introduce new ways of thinking. For many innovators, the only way to win an MoD contract is to sub-contract for a prime contractor. While the total quantity of MoD contracts illustrates a diversification of funds among SMEs, the truth is that most of these cover estate maintenance, basic electronics, clothing, training provision and so on, while most weapons-related contracts are concentrated among prime contractors. This raises concerns about a lack of competition and the impact this has on quickly addressing critical needs and capability gaps. While the MoD is comfortable with this arrangement, it is likely to feed a self-defeating cycle of cost overruns, delays and innovation stagnation.

Aside from a significant cultural shift, there are practical steps that the MoD can take to boost the participation of startups and new entrants. First, it can increase partnerships and communication with the startup ecosystem. At present, privileged access to MoD capability needs and technical requirements resides with well-established prime contractors, who often have the strongest relationships with the MoD. Second, it can simplify the labyrinth of procurement requirements, protocols, procedures and standards that are at best dissuading and at worst preventing small companies from participating. This includes, for instance, security-clearance challenges, which Air Street Capital articulated;[78] at present, companies need security clearance to win contracts but cannot win contracts without security clearance.

Here the UK can learn from approaches in the US, such as the role of In-Q-Tel, a not-for-profit venture-capital firm contractually linked to the CIA. The firm invests in information technology to support US capability needs, as well as acting as a go-between for small companies and the US government.

THROUGHWAY: THE PROCUREMENT PROCESS

In addition to crowding in defence innovators, the MoD needs to realign its procurement and development processes to meet the capability needs of today's fighting force.

The UK defence system needs to reorient its focus on procuring for the armed forces, with the armed forces. This requires a ruthless focus on identifying user needs and, whenever feasible, bringing in those who fight wars to work alongside industry to research, build, test and validate solutions

together. The UK can pull examples from the US Joint Special Operations Command for user-centred procurement. Ukraine's Brave1 model, a digital platform through which companies and startups can pitch ideas and products for state grants, also offers lessons for testing and prototyping. Similarly, Estonia's CR14 unit, a foundation offering virtual environments for cybersecurity exercises, demonstrates the potential for simulation training and modelling.[79,80] Each of these approaches finely illustrates newer and more adaptive methods of procurement to meet the dynamic demands of the 21st century.

Drawn out and inflexible budgeting processes are hindering the MoD's ability to keep pace with evolving technologies and threats. MoD budget planning takes place in multi-year cycles, which means the military is currently budgeting and planning for several years ahead. And once budgets are approved and passed, there is very little flexibility to move funds to different accounts to change how they are used. These factors are entirely unsuited to enabling a flexible and adaptable fighting force. When compounded by the immensely slow procurement process for new weapons and systems, which also takes years, the result is that many new capabilities or systems will be outdated or even obsolete by the time they come online.

The future of war is changing the definition of "power". Supremacy on the battlefield is less about raw firepower and more about information, networks and integration. This is also demonstrated in Ukraine, through its mesh networks of civilian and military sensors, integrated and automated command and control (for example, GIS ARTA), and the integration of autonomous systems into tactical operations.[81] Making this shift means focusing less on a single capability or system and more on building an integrated and networked defence apparatus – and bringing it together within a modular open-system architecture.

MoD procurement is far too focused on hardware, despite the central role of software in countering hybrid threats and enabling modern weapons systems. Defence acquisition is still rooted in the concept of buying a physical piece of hardware – a tank, an aeroplane or munitions. But the reality is very different: software underpins nearly every aspect of a modern military, with AI, mesh networks and autonomous systems serving as central components of a ready and capable military. Software is dynamic and needs continuous updates and security patches, something unaccounted for in traditional

defence-procurement systems.

The AI arms race is rapidly advancing, as are efforts to incorporate AI into military operations that are well underway; therefore, the MoD adapts procurement teams and processes to these shifts. UK Minister for Defence Procurement James Cartlidge admitted in a defence-committee hearing in March 2024 that while progress on AI adoption within the MoD is good overall, in predictive maintenance, for example, it has not yet reached the highest levels of preparedness in all areas. The MoD urgently needs to address this gap by adopting agile and adaptive procurement mechanisms for AI technologies that integrate the lessons learned from equipment supplied by UK SMEs to the Ukrainian theatre. This also includes staffing procurement teams with technologists and those who fight wars, following agile and flexible procurement models. Experimenting with other procurement methods is also crucial – including, for instance, contractor-owned, contractor-operated (COCO) models – to help address short-term pull-through capability shortfalls and field test new technology faster.[82]

The MoD should further integrate AI to automate procurement functions and better utilise big data. In a highly bureaucratic agency such as the MoD, AI can streamline and simplify processes to reduce manual workloads and improve the experience for, and feedback loops from, the vendor community. In the US, both the army and air force are exploring the integration of AI solutions into their procurement process. This includes an AI bot to reduce report generation from more than an hour to less than five minutes[83] and an AI-powered programme to support contracting officers in quickly searching and navigating procurement rules and regulations, respectively.

INNOVATION UNITS

With only a few viable entry points into defence contracts, new market entrants and non-traditional contractors are rare – and innovation in the UK defence sector is suffering as a result. Where innovation is happening, small batches of funding are failing to translate into sustainable purchase orders, let alone scaled and deployable technologies.

The unfortunate reality is that current UK defence-innovation units are set up to fail, in large part because they are patched onto a broken system, with minimal funding, insufficient expertise and a lack of political capital. There is a lack of appetite for trying new things within the MoD, which means

organisations such as (Defence and Security Accelerator) DASA and jHub, the UK Strategic Command's innovation team, end up with many exciting new research and prototype capabilities, but very little pull-through capability to large contracts.[84], [85] This leads to precarious results for young or small companies looking to secure larger funds to scale their products or prototypes. At the moment, the system seems to function merely to increase the cohort of specialised companies sub-contracting for the same primes, instead of actually expanding the number of smaller defence-innovation contractors.

The level of funding dedicated to these units is not fit for large-scale innovation. In fiscal year (FY) 2022, DASA received £49.1 million in funding.[86] In comparison, in FY 2022 the Defense Advanced Research Projects Agency (DARPA) in the US received $3.8 billion, nearly 77 times DASA's funding.[87] The US Defense Innovation Unit saw similar budget jumps from $43 million in FY 2022 to $112 million in FY 2023. The UK is hard-pressed to grow an innovation ecosystem based on a series of £50,000 R&D grants that may or may not end in contracts; companies cannot build a business model on these minimal grant cycles. This results in a lack of power to get technology to the front line at scale.

Modernisation of NATO procurement is critical to enhancing the alliance's operational capabilities. It will also play an important role with regard to US politics, both in terms of showcasing NATO's monetary and capability value add, as well as filling a potential capability gap left behind by the US pivot to Asia. These efforts must build upon NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (NIF) to further increase support for early-stage defence tech. That could include expanding the remit of both DIANA and NIF beyond dual use to invest in startups with direct defence applications, such as autonomous weapons systems.

Furthermore, modernising NATO procurement should include using the Joint Expeditionary Force (JEF) as a vehicle to go further and faster on AI procurement, with a "JEF Digital" initiative, proposed by RUSI, whereby startups from across the ten participating countries could pitch, design and test military applications of AI for JEF countries to deploy. This would require greater cooperation across JEF countries on data access, transfer and storage, but would create a pooled data resource that could also act as a backup if NATO data systems are destroyed in a conflict.[88]

Lastly, the UK must also increase defence-innovation cooperation with the European Union. As TBI has previously proposed, the UK and the EU should explore a European defence-capability review to identify collective asset and capability shortfalls.[89] If the UK concludes a broader defence and security agreement with the EU, full participation in EU defence-procurement initiatives, such as the European Defence Fund, could also be unlocked.[90]

THE OFF-RAMP: STRENGTHENING PULL-THROUGH CAPABILITIES

In today's dynamic and tech-driven threat landscape, investments made to diversify industry partners and early-stage R&D must be met with equal efforts to procure, manufacture and field those technologies at pace and scale. Unfortunately this is not the case in the UK: pull-through capabilities within the MoD remain a critical point of failure. Too often, well-intentioned prototypes and pilots do not end in an MoD contract. The UK must create better symbiosis and pull-through capabilities from research to production, or the "off-ramp", by addressing the funding gap for late-stage R&D.

The lack of pull-through capability is the biggest point of failure in the defence-innovation ecosystem, and must be thoughtfully addressed to ensure innovation funds and research grants actually deliver capabilities to the armed forces. Currently, innovation units such as DASA are allocated small sums to fund R&D and early-stage prototyping, but those initiatives are rarely purchased and scaled by MoD procurement. This creates a graveyard of good ideas and innovations killed off by a lack of longer-term funding. Without addressing the off-ramp challenge, small-scale innovations (and companies) will continue to disappear without ever seeing the light of day.

The "Valley of Death", the lag period between prototyping and funding, affects many startups trying to do business with the MoD. Typically a company, startup, research organisation or university will receive a grant to conduct research or develop a prototype. When the first phase of the project completes, the large-scale funding from the MoD is not secured to transition that technology into a scalable product. This lag period can last between one and three years, and is the period in which most new defence ventures fail. In many cases, the issue is not a lack of interest but the amount of time it takes to secure funding.

The UK should look to US efforts to close this gap, including Accelerate the Procurement and Fielding of Innovative Technologies (APFIT), a pilot

programme that aims to finance innovative and mature technologies that lack funding to transition into production phase,[91] and the Small Business Investment Company Critical Technologies Initiative (SBICCT), launched in 2022 as a joint venture between the Department of Defence (DoD) and the Small Business Administration. SBICCT aims to "scale public-private partnered capital and catalyse investment in critical technology areas".[92]

Venture capital (VC) can play an instrumental role in both bringing companies into the defence sector and bridging the funding gap. The VC ecosystem in the US is a useful illustration of how this can work in practice, by both creating more synergies between startups and the military, and helping the former bridge funding gaps as required to scale new technologies. This is particularly true for dual-use technologies. The need for more defence-innovation funding is clear, yet the UK defence VC ecosystem pales in comparison to the US.[93] This trend holds true across Europe, including an all-too-common set of stipulations within investor agreements that restrict VCs to investments in dual-use technologies, excluding defence-only technologies and solutions.

A NATO bank would also support pull-through by helping European countries invest more in defence. As a number of defence experts have argued, an allied multilateral lending institute would almost certainly be awarded "triple A" credit status, allowing NATO countries with lower credit ratings to borrow for defence investment at lower interest rates over longer time frames.[94] The bank would also support interoperability and send demand signals to the defence industry, delivering confidence for greater production. This idea was considered in 2019, but low interest rates led countries to decide that political concerns around collective debt outweighed the positives. NATO must reconsider this idea and if progress is not forthcoming, the UK and other JEF countries should consider RUSI's proposal for a JEF to act as a stepping stone towards this objective.[95]

PRODUCTION CAPABILITIES

In addition to modernising procurement processes and funding off-ramps, the MoD must develop an adaptable and strategic production sector to meet increased demand and achieve the necessary specialisation of defence innovation. Without robust and aligned production infrastructure, achieving widespread innovation will remain a formidable challenge. The

current system's limitations in meeting production capabilities for all weapons necessitate a strategic approach to prioritising which capabilities are most crucial.[96]

First and foremost, the MoD must focus on bending the cost curve back on traditional weapons systems and munitions, and new defence innovations. Capability development over the past few decades has focused on a handful of complex platforms, such as submarines, bombers and anti-aircraft systems. But this reliance on costly, complex and singular systems poses adaptability and resilience challenges. The staggering disparity in cost between adversary threats and allied responses is unsustainable. In Yemen, for instance, the US Navy shot down 38 drones and multiple missiles in the Red Sea over a two-month period in late 2023, with Houthi drones costing around $2,000 and US missiles adding up to more than $2.1 million dollars per shot.[97] In many circumstances, the same outcome can be achieved by better utilising dual-use tech and foregoing the urge to create unit-specific, bespoke and overly specialised weapons systems.

In support of prioritising cost-effective deterrence overseas, the UK needs to focus on identifying and ramping up mass-produced, low-cost capabilities. More specifically, this means a pivot in procurement and production toward "affordable mass" – cheaper, expendable, networked systems, with the ability to swarm to increase their effectiveness – to counter threats and project power through a forward presence across multiple theatres at once. As the war in Ukraine has illustrated, off-the-shelf drones are highly effective and adaptable to various missions.

At the same time, it must be understood that some missions cannot be conducted with mass-produced, low-cost systems. Particularly in the air and at sea, the physics of energy density and propulsive efficiency, as well as environmental stresses inherent in the operating environment, mean that some tasks (especially those that involve operating over great ranges or at great speeds) will continue to require exquisite, bespoke platforms, specialist crews and weaponry.

NATO's Defence Production Action Plan is a step in the right direction. Agreed last year, the plan focuses on combining large equipment orders to provide industry with clear and predictable requirements, creating a new Defence Industrial Production Board to share best practice, and increasing interoperability, with an initial focus on land munitions.[98] But as former Head of

NATO Innovation Rob Murray has warned, more action is needed to ensure the plan's success, particularly on awarding contracts and agreeing standards more quickly.[99]

This challenge is particularly salient for the war in Ukraine, as arms manufacturers grapple with the challenge of maintaining a steady flow of materials amid a relentless war. According to NATO intelligence, Russia is producing three times as many artillery shells as the US and UK are able to produce together for use in Ukraine annually. Russia is producing nearly 250,000 shells per month, or about 3 million per year. The UK and US collectively have capacity to produce about 1.2 million per year.[100]

And it is not just Ukraine: a global shortage of munitions makes UK action all the more imperative. Analysis by the Center for Strategic and International Studies suggests that in the event of a conflict over Taiwan, the US would run out of some forms of munitions in less than a week.[101] If such a conflict were to coincide with a Russian attack on NATO, Europe would be unable to rely on American munitions. The EU has been unable to meet its pledge of delivering 1 million artillery shells to Ukraine within a year.[102]

The UK and the West must therefore develop the capability to surge munitions production – not just to ensure their own security, but to shore up their ability to support other countries under attack, and to deter aggressors. A strong industrial base across the economy generally, which can be diverted towards defence production in the event of a war, will be critical to achieving this – as it has been in previous large-scale conflicts. TBI recently published a report on this subject: *Accelerating the Future: Industrial Strategy in the Era of AI*.

There are a number of challenges to securing munition supplies, not least the necessary level of investment. As the House of Commons' Defence Committee has reported, there are also significant logistical challenges, including production lines being squeezed by a shrinking list of buyers, supply-chain bottlenecks, a lack of investment in new production facilities and staffing shortages.[103] Furthermore, a number of experts consulted for this paper have warned that Treasury spending rules around ammunition stockpiling have been another barrier to maintaining effective production. The government's recent commitment to spend £10 billion more on munitions production over the next decade would help address the investment problem – if this funding can be sustained.[104]

A resilient supply chain underpins these production capabilities and the UK's ability to maintain overall military readiness, especially during times of heightened tensions such as those that Europe is currently experiencing. However, the pandemic put the resilience of the UK's defence supply chains into question, which will only be further disrupted by rising geopolitical tensions, energy woes, budgetary constraints and the looming prospect of conflict. As the 2022 UK Defence Supply Chain Strategy (DCSC) rightly highlights, a strategic shift is needed to forecast threats and potential disruptions, and in-depth engagement and information sharing with the commercial sector are required if UK defence supply chains are to continue to insulate themselves from external shocks and stressors.[105] Given the increasing importance of AI for warfare, the UK must also seek to build sovereign supply chains for semiconductors. If necessary, this should be done through state subsidies, as proposed in a previous TBI report: *A New National Purpose: AI Promises a World-Leading Future of Britain*.

Recommendations in Review: Procurement

THE ON-RAMP

- Invest in developing new partnerships with industry and deepening existing ones, with a focus on startups, SMEs and non-traditional contractors, as well as academia, national labs and research institutes.
- Establish an agency or department to facilitate these partnerships. This should follow the model of In-Q-Tel, and act as a go-between for small companies and the MoD, helping those companies navigate the procurement process.
- Overhaul and simplify the procurement "on-ramp" by, for example, lowering bureaucratic barriers to entry (where security permits) to crowd in a more diverse defence-innovation base. Look to the US DoD's Defense Innovation Unit for examples for simplified solicitations, and employ AI to expedite the process for the MoD and vendors.
- Modify security-clearance processes for startups to mirror processes for contractors and MoD personnel, allowing startups better and direct access to defence contracts, instead of having to support the work of a larger prime contractor.

THROUGHWAY: THE PROCUREMENT PROCESS

- Broaden the threshold for exemptions to facilitate the advancement of defence technology, like the use of Other Transaction Authorities in the US. Striking a balance between a necessary level of risk aversion and a push towards experimentation and speed is essential to drive the development and adoption of new technologies.
- Whenever possible, bring armed-forces personnel into the procurement process using a co-design, co-build model to jointly develop, test and iterate on solutions for the end user, with the end user.
- Develop new software-acquisition standards or a playbook to improve software acquisition and procurement. Invest in education and training programmes on AI and other emerging software technologies.
- The MoD should also ensure efforts proactively take into account NATO's "Responsible AI" certification standard, which is currently being finalised and aims to translate NATO's 2021 Principles of Responsible Use into concrete checks and balances for the deployment of AI in the alliance.
- Invest in AI-powered tools to automate and streamline the procurement process. The adoption of smart tools can reduce manual workloads and lead to improved supplier relationships, better risk management and valuable insights for decision-making.

Innovation Units

- Increase funding for both DASA and jHub by at least £50 million per annum. If the UK wants to take defence innovation seriously, it must back up those efforts with investments in its existing MoD innovation hubs.
- Appoint a private-sector tech expert as director of DASA and hire a similarly expert, specialist team. Elevate that director to report to the secretary of state for defence. Bringing in a technologist (who can work private-sector speed and agility into the innovation process) and elevating the reporting structure builds political buy-in and synergies between the innovation hubs and the MoD procurement machine.
- Set up a defence-technology forum, chaired by the new director of DASA and consisting of tech SMEs with defence applications. Meeting regularly, this forum would bridge public procurement and private technology enterprise, increasing the tech sector's knowledge of capability requirements and DASA's knowledge of capital requirements.
- Expand the remit of DIANA and NIF to invest in startups with direct defence

applications, as well as dual-use applications. Set a DIANA "challenge" for increasing modular design and 3D printing of munitions.
- Set up a "JEF Digital" initiative for startups to pitch, design and test military applications of AI for JEF countries to deploy.
- Explore a joint UK-EU defence-capability review to assess collective assets and capabilities, including respective gaps and shortfalls, and the UK's potential participation in the European Defence Fund.

The Off-Ramp

- Establish a defence accelerator unit, backed by ample funding, aimed at quickly scaling and fielding new technologies. This programme should aim to 1) increase the transition of dual-use commercial technologies, with a particular focus on UK defence innovators, and 2) augment the funding and transition capabilities of DASA and jHub projects. NATO should look to establish a similar programme.
- Establish a NATO or JEF bank to support countries in investing more in purchasing and scaling innovative new defence capabilities.

Production

- Identify priority capabilities over the next five to ten years and ruthlessly prioritise investment and production capacity for them. This should be done in coordination with industry and key allied nations.
- The US, UK, Australia and other key NATO partners should renew their focus on "allies by design", integrating a cooperative and collaborative approach to procurement and production of weapons and systems.[106] This means procuring systems and weapons that augment, rather than duplicate, allied capabilities.[107]
- Invest in partnerships with industry. This entails close collaboration to align production needs with existing capabilities, plus long-term assured contracting and communication and coordination, to guarantee timely delivery of critical resources.
- Establish an initiative to scale mass production of low-cost, expendable systems, with a focus on autonomous and networked weapons systems. This could mirror the US Replicator Initiative, which will receive up to $1 billion in DoD funding in 2024–25,[108] and aims to "... create on-ramps for new capabilities, systems and commercial partners that fill both operational and scaling gaps with available resources".

- Build on the NATO Defence Production Action Plan[109] by:
  - Speeding up contract awards through a new streamlined process that focuses on smaller, more frequent contracts.
  - Accelerating the process of standards development by involving producers more directly in the standards-development process.
  - Negotiating the creation of a NATO tech-access clearing centre, as proposed by the Center for European Policy Analysis, "focused on dual-use exports, tech transfer, research protection, and creating a shared certification system for trustworthy vendors".[110]

08

New Types of Warfare Require a Different Mix of Personnel

The technological innovation witnessed in Ukraine's defence against Russia has also highlighted a need for different types of military personnel to complement more traditional pre-existing forces. Ukraine's newest fighting group serves as a good example of personnel innovation. In February 2024, reacting to the large increase in the daily use of unmanned aerial vehicles in the war, Ukrainian President Volodymyr Zelensky announced the creation of a separate armed-forces branch focused on drone warfare. Drone operators, particularly those in Ukraine operating first-person-view drones with shorter range, require different skills to traditional armed-forces personnel. They must combine fieldwork and technical skills with an understanding of AI and its impact on the battlefield.

To use the UK as a specific example, in 2021, following an integrated review, the British Army published a "Future Soldier" strategy [111] that highlighted the ways in which the country's armed forces would need to adapt to both new capabilities and their own newly reduced size, the latter a consequence of decreased spending and diminished interest in serving in the armed forces. While making better use of technology will be critical for the UK's defence capabilities, this cannot come at the expense of maintaining the capability to deploy boots on the ground. The next government must rethink this strategy to avoid an over-reliance on technology.

The National Security Team must pursue a defence-and-security strategy that makes better use of emerging defence capabilities while maintaining the ability to deploy troops. This will require action in three areas.

BUILDING NEW SKILLS FOR NEW CAPABILITIES

The UK needs more people with skills in science, technology, engineering and mathematics (STEM), and expertise in technology, to join its defence ecosystem, in particular the armed forces. The MoD has warned that the armed forces suffer from significant shortages in engineering, communications, cyber and medical skills, while the 2023 Haythornthwaite

Review of Armed Forces Incentivisation concluded that "rising demand for skills is already not being met in some key areas, including cyber, engineering, nuclear, digital, logistics, aviation and medical."[112],[113] Meanwhile, venture-capital firm Air Street Capital has warned that a lack of tech expertise within the MoD is hampering the country's procurement of cutting-edge AI for defence.[114]

Doing more to attract women into the armed forces would help fill operational pinch points such as engineering and cyber. While men still constitute a majority of STEM learners, recent statistics show that women make up a sizeable minority of higher-education students in mathematical sciences (37 per cent), computer sciences (23 per cent), and engineering and technology (21 per cent).[115] With women making up only 12 per cent of armed-forces regulars and 15 per cent of officers,[116] increasing the appeal of the armed forces to women would help fill STEM-skills gaps. To help achieve this, ministers should appoint a Women's Defence Champion to showcase the opportunities for women who work in the sector.

The UK needs to address STEM-skill shortages across the economy. When recruiting STEM graduates, the armed forces and defence sector are competing with multinational companies such as Google and Meta, which are able to offer significantly more pay. Increasing the number of STEM graduates will help increase the pool from which the defence sector can recruit, as well as benefitting other areas of the economy. While reforms to education are beyond the scope of this paper, the next government should consider proposals put forward in previous TBI reports such as *A New National Purpose: Innovation Can Power the Future of Britain*.

As former US Under Secretary of Defense for Policy Michèle Flournoy has argued, Western countries need to restructure their armed forces to bring tech expertise to the fore.[117] This will require changes to how training in digital capabilities is delivered. All armed-forces training should cover basic digital capabilities, while the UK's Defence Cyber Academy could be expanded into a broader Defence Digital Academy that provides specialist personnel with training covering a range of cutting-edge technologies, from cyber to AI.[118]

The UK should also seek to attract individuals with more advanced tech skills into the armed forces through higher pay and increased awareness of opportunities. In this vein, the UK should also address the specific challenges facing individuals in service and highlight the positive role that its

armed forces play in society.

Increasing awareness of the opportunities that work in the defence sector offers to use STEM skills is also critical. A 2021 survey of 18- to 25-year-olds interested in STEM roles found that two-fifths of respondents were not aware that these kinds of opportunities were available within the armed forces. Once presented with a list of roles, the proportion of respondents who said they would consider a STEM career in the armed forces increased significantly.[119]

Even when people are aware of these opportunities, perceptions of defence can act as a barrier to recruitment. The same 2021 survey found that many respondents were not interested in armed-forces roles due to "the ethics of working for the military, being away from family or feeling uncomfortable or unwelcome in the armed forces". YouGov polling from 2023 shows that compared to the population as a whole, 18- to 24-year-olds are half as likely to hold "very favourable" views of the army.[120]

To overcome these barriers to recruitment, specific challenges in the armed forces must be addressed. As discussed in the next section, satisfaction with the services has declined significantly in the past 15 years, and interventions are needed on food and housing quality to make the prospect of serving in the armed forces more attractive.

Furthermore, sexual harassment in the armed services needs to be tackled as a matter of urgency. Sarah Atherton's 2021 report on women in the armed forces found that servicewomen were more than ten times as likely as servicemen to experience sexual harassment. Earlier this year she warned that since her report was published, ministers have only "taken the low-hanging fruit … and the more difficult issues are yet to be addressed".[121] Aside from the moral duty of the government and armed forces to prevent these crimes against servicewomen and hold perpetrators to account, the prevalence of these crimes is bound to dissuade many people from joining the armed forces.

Action is required to highlight the positive role that UK armed services play in society and rebut narratives that supporting the defence sector or serving in the armed forces is unethical. Actioning the Hawthornthwaite Review's recommendations on creating a single tri-service team to expand younger people's awareness of the armed forces, and using social media and real-life networks to reach more young people, would be a step in the right

direction.[122] More work is needed on awareness and perception, starting earlier, with a focus on underrepresented groups.

The National Security Team should seek to expand school cadet forces as another way to challenge negative perceptions of the armed forces. In 2012, the government's Cadet Expansion Programme set out to increase the number of cadet units in state schools, with a focus on deprived areas, and succeeded in more than doubling the number of schools with units. A 2021 study also showed that cadet schemes disproportionately benefit those from deprived backgrounds, improving school attendance, mental health and social mobility.

The next government could consider reforms to the national curriculum in order to highlight the important role that the armed forces play in protecting the UK and its liberal-democratic values. At present, England's national curriculum for citizenship for Key Stages 3 and 4 does not explicitly mention the armed forces, despite the subject's focus on society, values and institutions.[123] A 2022 report written by a group of experts in education and skills rightly recommended that citizenship education "be reinvested in and expanded upon"; a greater focus on highlighting the role of the armed forces in protecting society and values could also be prioritised here.[124]

Action is also needed to upskill existing defence personnel with tech skills. Again, the Haythornthwaite Review's recommendations for upskilling and reskilling current members of the armed forces pull in the right direction. The review's proposals for a Personal Digital Profile for personnel, and adoption of the Australian model of testing and reviewing aptitudes early in recruits' careers, will make it easier to upskill and reskill members of the armed forces as requirements develop for different capabilities and skills in response to emerging technologies.

The National Security Team should ensure that more is being done to give civil servants at the MoD experience at the cutting edge of emerging defence technology. As Michèle Flournoy has argued, this is particularly important for government professionals responsible for procuring defence software; she has previously called for a "Green Berets of acquisition" in the Pentagon.[125]

The best way to achieve this in the UK would be a secondment scheme modelled on the Shift Defense Ventures Program in the US. Before the

programme was discontinued in March 2024, it embedded active-duty and reserve officers and civilians from the US DoD in venture-capital firms and defence-tech startups for either an eight-week experience or a 12-month fellowship. A survey of participants by Shift found that 72 per cent of the fellows reported an increase in technology proficiency between threefold and tenfold, and increased understanding of industry best practices. Jake Chapman of US venture-capital firm Marque Ventures has argued that Shift's programme was "one of the largest catalyzing factors in what can be described as a revolution in civil-military affairs", as well as one of the contributing factors in VC investment in US defence tech more than doubling in the past five years.[126]

RECRUITING AND RETAINING

Since 2010, the trained strength of the UK's armed forces has been cut from 178,000 to 134,000.[127] The number of trained personnel in the army, which has been subjected to the largest cuts, has fallen from 102,000 to just 74,000 and, based on present recruitment and retention figures, is expected to fall below 70,000 within two years.[128]

These reductions can be attributed primarily to funding pressures and difficulty recruiting and retaining personnel. While funding pressures have been acute since 2010, the recruitment-and-retention problem can be traced back further: since the millennium there have only been six years in which recruitment to the regular forces has been higher than outflow. As a result, the army's trained strength has been below the required level for almost every year in the past two decades.[129]

The National Security Team must overhaul the recruitment system so that people who want to join the armed forces are supported in doing so. Since 2012, army recruitment has been outsourced to UK firm Capita under the Recruiting Partnering Project agreement, but the company has consistently failed to meet its targets. For instance, it was forecast to achieve just 70 per cent of its target for 6,800 regular soldiers in 2023–24.[130] While the Royal Navy and the Royal Air Force remain largely responsible for their own recruitment processes, they too have struggled to recruit the required number of personnel. But with only about one in ten applicants successfully entering the armed forces, the problem seems to be process rather than demand.

Around half of applicants to the army are rejected following failed medical

assessments. At present, applicants to the British Army have their GP-held medical records shared with Capita and are seen by another GP at an assessment centre, where they are assessed against definitive medical standards. In cases where Capita deems an issue to be marginal and in need of another opinion, the applicant is referred to a doctor within the armed forces for further assessment.[131]

Capita data show that the top three reasons for medical rejections for recruitment in 2022–23 all related to mental-health problems: two or more episodes of depression (1,011 candidates); other anxiety disorders (890); and two or more episodes of self-harm (687). However, Capita warns that even rugby players with high body-mass-index (BMI) scores from muscle mass or historic broken bones would struggle to join the armed forces.[132] A more holistic approach to assessing medical fitness for the armed services is needed.

Application delays are another serious concern. According to Capita, "the fact that it takes 150 days to join the army means that some of our potential recruits get attracted elsewhere because there is a speed to get a job that is higher elsewhere". Data from Labour found that last year, 54 per cent of people who applied to join the army withdrew their applications.[133] Capita suggests that checking for health issues is a significant part of this delay; the company is investing in AI that can help to check through medical records and make decisions faster.[134]

While it is right that the process seeks to ensure that only sufficiently healthy people serve in the armed forces, these data suggest that societal changes around mental health are having a disproportionate impact on recruitment. As decreasing stigma around these conditions has led to an increase in diagnoses, the recruitment requirements on mental health are acting to exclude people who previously would have been able to serve. That healthy people with high BMIs are being excluded is a further demonstration that tick-box exercises are not suitable for assessing whether a person is healthy enough to serve in the armed forces.

Given Capita's failure to meet its recruitment targets, the National Security Team should consider stripping the company of its contract. The outsourcing in 2012 was designed to release about 1,100 soldiers from recruiting roles, but Capita's failure to sign up enough new joiners led the army to move 400 soldiers back to recruitment offices in 2023.[135] As former army

officer and chemical-weapons expert Colonel Hamish de Bretton-Gordon has argued, those with experience in the armed forces are likely to be the best judges of whether an applicant is physically and mentally healthy enough to deal with the demands of service.[136]

In 2020, the Ministry of Defence set out plans to extend the current outsourcing recruitment approach for the British Army to the Royal Navy and RAF through a new tri-service recruitment contract: the Armed Forces Recruiting Programme.[137] While this was initially set to enter service in 2024, there have been significant delays, with the government now planning to award the contract in 2025 to begin in 2027.[138] While the recruitment challenges that other countries are facing show that Capita is not entirely to blame for the UK armed forces' current situation, the firm's performance raises questions as to the wisdom of further outsourcing.

After the general election, the government should review the planned Armed Forces Recruiting Programme, with a view to scrapping the contract unless clear, demonstrable evidence can be produced that shows further outsourcing will lead to a significant increase in recruitment. In the absence of such evidence, the Royal Navy and RAF should continue to lead their own recruitment services, and responsibility for army recruitment should be returned to the British Army as soon as possible.

Increasing the number of recruits is only half the challenge: retention is just as critical. Outflow from the regular forces in the British Army, RAF and Royal Navy has been greater than recruitment in seven of the past ten calendar years. In 2023, 16,100 personnel left the three services compared to the 10,700 personnel recruited, leaving a shortfall of 5,400.[139] Among trained regulars, voluntary exits accounted for 61 per cent of personnel outflow last year.[140]

Declining satisfaction with the services seems to be driving high rates of voluntary outflow. The latest Regular Armed Forces Continuous Attitude Survey data show that satisfaction with service life for non-officers was just 39 per cent last year, compared to a peak of 58 per cent in 2009.

The Haythornthwaite Review puts forward a number of valuable proposals for improving retention by upgrading the day-to-day aspects of life in the armed forces. These include: enhancing the choice and quality of subsidised food by expanding military dining scheme Army EATS; improving

accommodation quality by allowing commanders to spend up to £100,000 on improvements per financial year; and expanding the Forces Help to Buy Scheme to boost home ownership among armed-forces personnel.[141]

TAKING A "WHOLE-OF-SOCIETY" APPROACH

Alongside action to make sure that the armed services are war-ready, action must be taken to ensure that civilian society is adequately prepared for a serious conflict. As Ukraine's experience demonstrates, significant factors in a country's ability to fight a war are support among its population and the resilience of its people. In the event of a large-scale conventional war against a country such as Russia, the UK will only be able to succeed if it adopts a whole-of-society approach to defence, such as that employed by the Scandinavian countries. This will require action in three areas.

First, the pool of skilled people who can be called upon to perform military or civilian tasks in the event of a war must be expanded. The National Security Team must take action to train and recruit reservists to ensure that the reserve force has the skills and strength to be effective in a conflict. Since the establishment of the Joint Cyber Reserve Force in 2013, progress has been made on boosting reservists' skills.[142] And many of the options outlined above, such as reforming recruitment requirements and process, could increase not only the number of regular-forces personnel but also the number of reservists.

But there are a number of further options that the next government should consider to boost reserve numbers. For example, General Sir Patrick Sanders has proposed paying young people on gap years or waiting to go to university to take part in a month-long military boot camp, in the hope that they will then join the army reserves.[143] Ministers could also explore additional incentives to attract people with skills in high demand, such as cyber and engineering, via partial student-loan forgiveness. And the MoD could deepen its conversations with tech companies and university departments, as Michèle Flournoy has recommended in the US,[144] to better attract outside talent to the reserves.

Ensuring that the UK's Strategic Reserve of recent service-leavers can be called upon in a crisis will also be critical. The government's 2023 Defence Command Paper recognised this, emphasising the importance of the Strategic Reserve in generating "surge capacity and wider access to expertise in time of crisis or national emergency".[145] However, both media reports and defence experts consulted for this paper have warned that contact details for

recent service-leavers are not being recorded, meaning that many would be uncontactable in the event of a crisis.[146] The National Security Team must urgently review the extent to which these contact details are being maintained, and should introduce annual rehearsal exercises for the Strategic Reserve to ensure its members' skills can be effectively deployed in a crisis.

More action must be taken to leverage the skills of civilians for defence, such as maintaining and restoring key civilian infrastructure in the event of major disruption. The government has made some progress here, launching the Industry 100 scheme at the National Cyber Security Centre as a way to second people from industry to help identify systemic vulnerabilities and reduce the impact of cyber-attacks.[147] Ministers have also committed to creating a UK Resilience Academy by 2025 that will design and deliver training for resilience professionals.[148] Making a success of this academy will be key to guaranteeing that the UK has skilled civilians it can draw on in a crisis. As Elisabeth Braw of the Atlantic Council has argued, ministers must view Sweden's Civil Contingencies Agency (MSB) as a model for the UK Resilience Academy. The MSB offers training and exercises for organisations, public authorities and individuals to help them prepare for and reduce the impact of emergencies.[149]

Second, government needs to prepare for war and disruption. A former intelligence officer and advisor to Boris Johnson has warned that while working in government, he was unable to find any kind of detailed plan for war.[150] A former MoD minister claimed earlier this year that much of the civil service is uninterested in war readiness and has not prepared answers to difficult wartime questions, such as how to secure food or energy, produce weapons or maintain public services in the event of a large-scale war.[151] These reports contrast starkly with government preparations during the Cold War, when the UK had a 16-chapter Government War Book setting out precise plans for transitioning the country from peacetime to wartime, covering everything from food supplies to nuclear strikes.[152] Given this period of heightened geopolitical risk, the National Security Team must urgently prepare plans for various wartime scenarios.

Third, the British public themselves need to be prepared for war or massive disruption. Ministers have taken some steps forward here, launching a website offering guidance to help people prepare for different emergencies and committing to set up a volunteering hub that will help people offer their

skills and services in the event of a crisis.[153]

Existing proposals have the right ambition but must be delivered well to make a material difference, and the National Security Team should model its action in this area on the approach of Scandinavian countries. Sweden, for instance, aims to ensure that all households have the preparedness and supplies to survive for one week without any external assistance. Their MSB distributes a brochure entitled "If Crisis or War Comes" to every household in the country, with advice on how citizens can prepare to ensure they have access to food, water, warmth and communications.[154]

RECOMMENDATIONS IN REVIEW: PERSONNEL

- **Upskill personnel** by ensuring all military training covers basic digital capabilities and expanding the UK's Defence Cyber Academy into a broader Defence Digital Academy.
- **Implement the following Haythornthwaite Review recommendations** as quickly as possible:
  - Introduce skills-based pay elements, prioritising enhanced pay for STEM skills in pinch-point areas such as engineering, communications and cyber.
  - Create a tri-service team for building young people's awareness of the armed forces, and building links with social-media influencers who would be interested in working with the armed forces.
  - Set up Personal Digital Profiles for personnel and introduce the Australian model of early and regular aptitude testing, with a focus on identifying and recording aptitudes that suggest personnel could be successfully upskilled or reskilled to use emerging defence technologies effectively.
- **Appoint a Women's Defence Champion** to bring together existing networks of women serving in the armed forces and the defence industry, and to showcase the opportunities of working in defence for women in higher and further education.
- **Invest in increasing the number of community cadet units in state schools** and the number of participating pupils, with a focus on areas of higher economic deprivation.
- **Review the national curriculum for citizenship education for Key Stages 3 and 4**, to encourage schools to discuss the role of the armed forces in protecting the UK and its liberal-democratic values. Teaching materials on this subject can be commissioned from the Association for Citizenship

Teaching.

- **Work with venture capitalists and tech startups** to create a UK Defence Tech Secondment Scheme, to allow MoD civilians, and active and reserve officers, to upskill in emerging defence capabilities.
- **Design a more holistic approach to assessing medical fitness for the army.** Minimum health standards, particularly for mental health, should be relaxed for the initial screening procedure, so that only those with a history of the most challenging health problems are automatically excluded. Aa at present, applicants who pass the initial screening but may not be sufficiently healthy would then be referred by Capita for further assessment by a doctor in the armed forces. This new system would allow for greater subjectivity around certain health conditions, like mental-health conditions, while still ensuring that only the healthiest individuals are able to serve in the armed forces.
- **Launch a review to consider the effectiveness of the Recruiting Partnering Project** with Capita and reconsider plans for the forthcoming Armed Forces Recruiting Programme in 2027. As part of this review, ministers should consider returning ownership of recruitment to those with experience in the armed forces. To reduce the impact that this shift in responsibilities could have on the ability to deploy personnel, the government and armed forces could consider creating a corps of retired officers to lead on recruitment.
- **Explore ways to boost the pool of skilled people who can be called upon** to perform military or civilian tasks in the event of a serious war, including expanding the army reserves. The extent to which contact details for the Strategic Reserve are being maintained should be urgently reviewed, and annual rehearsal exercises should be introduced to ensure its members' skills can still be deployed in a crisis. The proposed UK Resilience Academy should be modelled on the Swedish MSB.
- **Set up a Wartime Preparation Taskforce** to prepare for the actions that the government's various departments and institutions would need to take in the event of large-scale conventional war. The taskforce's aim would be to produce a comprehensive internal plan for that eventuality, similar to the Government War Book of the Cold War period. It would be modelled on the successful Vaccine Taskforce and would consist of a small team of experts in defence and civilian resilience, led by an external expert who reports directly to the defence secretary.

09

The Right Alliances to Deliver the Right Strategy

This is an era in which, globally, only the two super-superpowers – China and the US – are able to project themselves militarily in a full-spectrum way. Even for these countries, important questions remain on how best to equip themselves with the right capabilities and keep those capabilities at the cutting edge. They will be able to draw on the right allies and alliances to expand their influence, but they will not be reliant on such relationships in the same way that other lesser powers will be. The UK can serve as a case study for the type of considerations that other countries must bear in mind when taking stock of an important aspect of their defence strategy: their formal alliances and focused strategic partnerships.

ASSESSING ALLIANCES AND ALLIES

The first step that a country should take when considering this aspect of its overall defence strategy is to conduct a thorough assessment of the state of its alliances and allies. This should cover not just the capabilities of the allies in question but how those capabilities interact with the ones that the country itself already has. The same is true in conducting capability assessments of alliances such as NATO: what does the alliance have the capability to deliver, and how does this align with the defence strategy the country has set?

These assessments should begin with current capabilities but should also map out future scenarios. Wargaming and scenario mapping of this kind will allow the assessment to not only clarify what allies or alliances are capable of now, but how these would meet future threats.

In the UK, this assessment should be carried out by the newly formed National Security Team in Number 10, with support from across government; the team would then build on this assessment to form the right coordination strategy with allies. A small unit within the team should be dedicated to this aspect of national-security strategy and should focus on assessing partnerships (and the UK's contribution to them) on an ongoing basis, working closely with allies and partners.

COORDINATING TO ENSURE VALUE-ADD

A country developing its defence-and-security strategy should be sure to do so in concert with allies, not in isolation. Assessing the capability of allies and alliances is important, as is the development of a national strategy that docks carefully into this assessment, but its practical impact rests on effective coordination with allies.

Take the UK, for example: a cornerstone of its defence policy is its relationship with European allies. The UK needs to work closely with partners in Europe to determine how its current and future defence capabilities as a country can best enable better collective capability. What joint projects could it work on with partners in Europe? Where can it develop deeper procurement relationships? How can it make sure that the areas it focuses on in its national security strategy will contribute to its wider collective defence?

The same is true of NATO. As a recent TBI article published in a British newspaper argued, in light of the new challenges NATO faces, the alliance's 75th anniversary this year should serve as an opportunity for renewal.[155] The next phase of NATO, as the US is increasingly drawn towards the Indo-Pacific, will need to be shaped and driven by Europe, so this renewal should be led by European partners. This will require increased spending by those partners – but also smarter spending. Renewing NATO to meet the challenges of the future requires not just more money but also better capabilities. Trump's comments on NATO, which raised concern about the US's commitment to the alliance should he win a second term, have triggered exactly this thinking among its members. The UK has a critical role to play to not only make sure that NATO has the right capabilities, but also that its own defence strategy is complementary to, and augmented by, the wider plan that the alliance develops.

AUKUS is another important example and has rightly been lauded as a model minilateral agreement to which other countries can aspire. This agreement between Australia, the US and the UK shows that with the right imagination and engagement, a small cluster of allies can work together to augment their own capabilities and global reach. AUKUS has quickly enabled the UK to enhance its tech and soft power on the world stage, and the US's commitment to reducing export-control requirements on military items by as much as 80 per cent for the UK and Australia will make the partnership even more effective going forwards.[156] So too would planned cooperation with

countries such as Japan and South Korea on R&D projects, as well as the potential integration of Canada into the partnership.[157]

For the UK, forming the right alliances will not only mean considering ways to deepen AUKUS, but also looking to establish similar formations that can further augment the country's capabilities and reach. The same principle applies to other countries, which can look to AUKUS-style groupings as a way to focus their own capabilities on their areas of strength, and to marry these with the complementary capabilities of allied countries with strategic geographic reach.

The JEF is another grouping that the UK must use to maximise its influence, specifically in Europe and the Arctic. Established in 2014 and led by the UK, the JEF is a military partnership between ten Northern European countries, designed for rapid responses and expeditions. As mentioned in "Emerging Capabilities Require New Procurement Processes", RUSI has argued that the JEF is an ideal forum for deepening military cooperation between NATO's northern-flank members and has proposed a number of recommendations for new JEF initiatives, such as a JEF bank and a JEF digital initiative.[158]

BEING AN EFFECTIVE ALLY IN AN EFFECTIVE ALLIANCE

Forming the right alliances is an important part of the right defence strategy for any country, but it is also important to be an effective ally.

This requires regular and ongoing engagement. The National Security Team would serve as an important additional tool that the UK can use to engage with partners and alliances. This would allow dynamic assessment of not just the threats that NATO faces, but the capabilities that the UK can provide and the role that it must play to contribute to an effective alliance.

Being an effective ally means being able to deploy forces and project capabilities. An essential part of planning the reimagined defence capability that the UK needs is armed forces that retain the ability to quickly and effectively deploy personnel. For example, the deployment of UK forces to the Balkans as part of wider UN, NATO and EU peacekeeping operations has played an important role in stabilising countries such as Bosnia and Kosovo.

This will require careful thought around consent for the deployment of troops. As part of the renewal of existing alliances and the establishment of new ones,

the UK needs to put clear mechanisms in place to allow the use of force and the deployment of troops. This will interact with domestic norms on the authorisation of the use of force but must also be clearly defined within the alliance itself. As part of its review of alliances, the UK must carefully consider the conditions under which the alliance would act, in what ways and with what mix of capabilities.

RECOMMENDATIONS IN REVIEW: ALLIANCES

- Conduct a comprehensive stocktake and refresh, led by the National Security Team, on the state of the UK's international alliances – bilateral, minilateral and multilateral. This should include an assessment of where the UK is able to contribute particular strengths, how these can be augmented by allies and what better coordination with these allies could achieve in terms of enhancing the UK's defence strategy.
- Set up a small, dedicated unit, with a full-time focus on alliances and international partners, within the National Security Team. The unit would provide ongoing assessment of the status of the UK's alliances, the UK's contributions to them and how they could be improved.

10

Conclusion and Recommendations

As this paper has set out, the complexity, threats and military capabilities that shape modern geopolitics are fast evolving. This context necessitates significant action by the government to ensure that the UK has the right strategy to navigate this new world.

In this age of geopolitical uncertainty and constantly changing risks, the centrality of national security to all aspects of government priorities requires new structures at the heart of government to better design policy, drive it from the centre, deliver it through the whole of government and ensure it is implemented.

The UK and its peers must carry out proper assessments of the capabilities required to prepare them for the changing nature of warfare. This will allow a better focus on what new capabilities are needed now, as well as those that are on the horizon. In a context where only the US and China are spending enough money to equip themselves for global projection on air, land and sea, other countries need to more carefully focus on identifying and deepening their areas of strategic strength.

New warfare capabilities are coming on to the front line at speed and, critically, are continuing to evolve quickly once there. This requires a radical rethink on how governments handle procurement: they must look for new ways to work with the private sector; improve their ability to procure within government; and establish a new framework to ensure that the right kit is procured from the right provider.

The emergence of rapidly developing technologies with defence applications necessitates an update on the type of personnel that the armed forces require. This will involve getting as many existing personnel as possible tech-trained, improving recruitment so that the right type of personnel can be hired for new roles within the military, and creating deeper and more dynamic links with the private sector to allow experts to more fluidly enter the public sector. All the while, the changing nature of war must be carefully assessed and the enduring need for traditional capabilities such as boots on the ground recognised.

If only the US and China can even begin to consider projecting their military strength unilaterally, every other country needs the right allies, alliances and partnerships to deliver their defence strategies. The UK will need to refresh and update which allies it draws upon, how it works with them and how these partnerships are constructed to guarantee delivering a security strategy that is worth more than the sum of its parts.

RECOMMENDATIONS

Strategy

- **A new National Security Team:** create a new team to reflect the importance of delivering a reimagined defence and security strategy that secures the country against a new era of threats. This team would be enhanced both in its role and in the type of personnel it recruits. It would give Number 10 the central capability to set, drive and continually evaluate the country's defence and security strategy.
- **A Centre for Strategic Futures:** establish this body as part of a new architecture to examine defence challenges now and in the future. This would sit outside government structures but report into the National Security Team; its key role would be to assess future threats beyond the horizon of the ongoing National Security Assessments. It would comprise recruits with a variety of backgrounds to bring long-term but also radical thinking: scientists, technologists, defence experts, diplomats, climate experts and so on.
- **Sustainable funding model for defence and security:** working with the prime minister and the National Security Team, agree a multi-year budget framework to provide the clear funding framework needed. An effective and sustainable national-security strategy requires consistent funding across a clear timeline to allow the right investment and long-term thinking. This budget would be reviewed by the National Security Team, working closely with the Treasury, so that new capabilities and opportunities can be seized.
- **New engagement mechanisms between private and public sectors:** hold monthly closed-doors sessions between the National Security Team and private-sector companies and representatives. For too long the state has interacted with the private sector in a way that serves neither well; this too often results in final tenders being issued without prior consultation with the defence industry and external experts. Closer and earlier

engagement is required. These proposed closed-door sessions would include horizon scanning, scenario planning and wargaming. This closer collaboration would allow the private sector to be engaged in assessments of the problems that the country faces on defence, rather than simply evaluating versions of the solutions shaped only by government. The strategic advantages group set up in Number 10 (under John Bew) made important strides in establishing this work, but it must be widened and deepened.

Capabilities

- **European sovereign capabilities:** conduct, with other European countries with advanced military capabilities, an urgent review to identify military capabilities where Europe is overly reliant on the US. Different countries should then agree on action to procure the most essential of these capabilities, complementing US strengths in the process and helping to plug any capability gaps that would arise from a reduction in support.
- **Counter-disinformation capabilities:** increase funding for the BBC World Service to combat disinformation in priority countries and regions such as Russia, the Balkans and the Middle East.
- **Satellite resilience:** invest in procuring more resilient satellite capabilities. One way to do this would be to support Eutelsat in launching a network of second-generation OneWeb satellites via UK Export Finance.
- **Seabed resilience:** work with allies to commission Western satellite companies to provide ongoing surveillance around critical seabed infrastructure, and to procure a greater number of underwater-surveillance drones.

Procurement

- **Defence accelerator unit:** establish a defence accelerator unit, backed by ample funding, aimed at quickly scaling and fielding new technologies.
- **Mass production of autonomous systems:** establish an MoD programme focused on mass production of low-cost, expendable systems, with a focus on autonomous and networked weapons systems.
- **Greater investment in defence R&D:** increase funding for both DASA and jHUB, at no less than £50 million more per annum. The MoD's budget for FY 2021/22 was £45.9 billion,[159] with nearly £30 billion[160] spent on procurement. If the UK wants to take defence innovation seriously, it must

deepen investment in its existing MoD innovation hubs.

- **Tech leadership at DASA:** appoint a private-sector technologist to lead DASA and elevate the director to report to the secretary of state for defence.
- **Investment in deepening partnerships with diverse industry stakeholders:** establish an agency or authority focused on strengthening industry partnerships and increasing the non-traditional contractor base. This could mirror an entity such as In-Q-Tel, acting as a go-between for small companies and the MoD, and helping smaller companies navigate the procurement process.
- **Accelerated experimentation of defence technology:** broaden the threshold for exemptions to facilitate the advancement of defence technology, like the use of Other Transaction Authorities in the US. Striking a balance between a necessary level of risk aversion and a push towards experimentation and speed is essential to drive the development and adoption of new technologies.
- **An "allies by design" approach to development:** institutionalise the joint development of certain weapons and systems, where appropriate, with a renewed focus on "allies by design",[161] integrating a cooperative and a collaborative approach to procurement and the production of weapons and systems.
- **Strengthened cooperation with the EU:** explore a joint UK-EU defence-capability review to identify collective asset and capability shortfalls, and the UK's potential participation in the European Defence Fund.
- **R&D cooperation through JEF:** set up a JEF Digital initiative, whereby startups can pitch, design and test military applications of AI for JEF countries to deploy.
- **Alliance banking initiative:** establish a NATO or JEF bank to support countries to invest more in the pull-through of new defence capabilities.

Personnel

- **Digital-capabilities training:** improve training for personnel in digital capabilities by ensuring that all military training covers the basics, and expanding the UK's Defence Cyber Academy into a broader Defence Digital Academy.
- **Defence Tech Secondment Scheme:** work with VCs and tech startups to create a UK Defence Tech Secondment Scheme, lasting up to a year, to allow MoD civilians and active and reserve officers to upskill in emerging

defence capabilities.

- **Reform of fitness-for-service requirements:** design a more holistic approach to assessing medical fitness for service. Medical records should be used to exclude only those with the most challenging health problems. Those with medical records suggesting some health challenges, such as a history of mental-health problems, should undergo an additional assessment by a member of the armed forces.
- **A new Wartime Preparation Taskforce:** set up a taskforce to prepare plans for the actions that the government's various departments and institutions would need to take in the event of large-scale conventional war.

Alliances

- **Alliance stocktake and refresh:** conduct a comprehensive stocktake of the state of the UK's international alliances – bilateral, minilateral and multilateral. This should be conducted by the National Security Team, which should assess where the UK is able to contribute particular strengths, how these can be augmented by allies and what better coordination with these allies could achieve in terms of enhancing the UK's national-security strategy.
- **Alliances and international-partners unit:** establish a dedicated unit, within the National Security Team, with a focus on alliances and international partners. This would provide ongoing assessment of alliances, the UK's contribution to them and how they could be improved.
- **Refresh wider capabilities on diplomacy and development:** align defence policy more closely with diplomacy and aid spending, while situating both within the capabilities of the UK's allies and alliances.

11

Acknowledgements

During the research and drafting phases of work on this paper we spoke with a range of experts and stakeholders. Their invaluable insights helped shape the report. We include below a number of the people we spoke with and thank them for their input.

Michèle Flournoy, former US Under Secretary of Defense for Policy

General Sir Nick Carter, former Chief of the Defence Staff

Michael Brown, Partner at Shield Capital, former Director of the U.S. Defense Innovation Unit

Andrew van der Lem, Head of Faculty Defence Team, Faculty AI

Alex Chalmers, Platform Lead, Air Street Capital

Kelly Grieco, Senior Fellow, Reimagining US Grand Strategy Program, Stimson Center

Professor Justin Bronk, Senior Research Fellow, Airpower & Technology, RUSI

Dr Jack Watling, Senior Research Fellow, RUSI

Shashank Joshi, Defence Editor, *The Economist*

Raphael S Cohen, Senior Political Scientist and Director of Strategy and Doctrine Program at RAND's Project Air Force

Erik Kannike, Chief Strategy Officer at SensusQ

Col (Ret.) Dean M Hoffman IV, President and Co-Founder, Accel Innovation Corporation

Dr Agnieszka Lukaszczyk, Vice President, Government Affairs, EMEA at Planet

Jon Williams, Founder of Allied and former Royal Marine

Sam Cash, General Partner, Entropy

Hamish de Bretton-Gordon, military analyst and former army officer

Peter Quentin, RUSI Associate Fellow, former policy adviser to Ben Wallace

Kata Escott CB, Managing Director, Airbus Defence and Space UK

Endnotes

1 https://power.lowyinstitute.org/data/military-capability/defence-spending/military-expenditure-defence-sector-ppp/

2 https://www.ssga.com/international/en/institutional/ic/insights/gmo-2024-macro-outlook

3 https://www.aljazeera.com/news/2023/2/16/mapping-where-every-country-stands-on-the-russia-ukraine-war

4 https://www.washingtonpost.com/national-security/2024/04/15/iran-israel-russia-drones-missiles/; https://www.reuters.com/business/finance/iran-russia-link-banking-systems-amid-western-sanction-2023-01-30/; https://www.reuters.com/world/us-asia-allies-push-new-panel-monitor-north-korea-sanctions-2024-04-17/

5 https://foreignpolicy.com/2023/11/29/axis-of-evil-russia-china-iran-north-korea-bush-era/

6 https://unctad.org/news/global-trade-expected-shrink-nearly-5-2023-amid-geopolitical-strains-and-shifting-trade

7 https://www.sipri.org/sites/default/files/Data%20for%20all%20countries%20from%201988%e2%80%932020%20in%20constant%20%282019%29%20USD%20%28pdf%29.pdf

8 https://www.institute.global/insights/politics-and-governance/new-national-purpose-innovation-can-power-future-britain

9 https://www.gov.uk/government/publications/dstls-divisions/exploration-division

10 https://www.bbc.co.uk/news/uk-68355395

11 https://www.bbc.co.uk/aboutthebbc/documents/ara-2022-23.pdf

12 https://www.bbc.co.uk/news/entertainment-arts-68654318, https://www.ft.com/content/12be030f-b4da-401b-adb4-2c5588a8bcb2

13 https://www.ft.com/content/b5987c48-cdb1-44f9-bf9c-55f6fe20ba12

14 https://www.ft.com/content/5953405f-d91a-4598-8b6b-6345452ca328

15 https://committees.parliament.uk/writtenevidence/129955/pdf/

16 https://committees.parliament.uk/writtenevidence/129955/pdf/; https://www.rusi.org/explore-our-research/publications/occasional-papers/requirements-command-and-control-uks-ground-based-air-defence

17 https://www.rusi.org/explore-our-research/publications/commentary/europe-must-urgently-prepare-deter-russia-without-large-scale-us-support

18 https://rusi.org/explore-our-research/publications/commentary/trump-proofing-nato-2-won't-cut-it

19 https://warontherocks.com/2020/12/how-the-army-out-innovated-the-islamic-states-drones/

20 https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/; https://www.bbc.co.uk/news/world-europe-68477318

21 https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/

22 https://www.gov.uk/government/news/new-uk-strategy-to-deliver-drones-to-armed-forces; https://breakingdefense.com/2024/01/no-contracts-yet-uks-plan-for-thousands-of-drones-for-ukraine-in-very-early-stages/

23 https://www.royalnavy.mod.uk/news-and-latest-activity/news/2022/june/17/220617-royal-navy-stormcloud

24 https://eccri.eu/wp-content/uploads/2023/04/ECCRI%5FREPORT%5FThe-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf

25 https://www.ft.com/content/a477d3f1-8c7e-4520-83b0-572ad674c28e

26 https://www.lemonde.fr/en/europe/article/2023/04/03/the-rise-of-cyberattacks-in-europe-amidst-the-war-in-ukraine_6021493_143.html; https://www.bloomberg.com/news/newsletters/2023-11-15/russia-s-sandworm-linked-to-unprecedented-danish-energy-hack

27 https://www.reuters.com/technology/cybersecurity/apt31-chinese-hacking-group-behind-global-cyberespionage-campaign-2024-03-26/

28 https://www.reuters.com/world/chinese-hacking-campaign-aimed-critical-infrastructure-goes-back-five-years-us-2024-02-07/

29 https://www.bbc.co.uk/news/business-68476035

30 https://www.bbc.co.uk/news/world-us-canada-68186945, https://www.france24.com/en/middle-east/20240214-iran-hackers-interrupt-uae-uk-canadian-programming-fake-ai-news-cyber-attacks

31 https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas

32 https://www.wired.com/story/generative-ai-terrorism-content/

33 https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure/#:~:text=The%20attack%20on%20the%20Nord,critical%20infrastructure%20on%20the%20seabed.

34 https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/

35 https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466?mod=article%5Finline

36 https://policyexchange.org.uk/publication/from-space-to-seabed/

37 https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/

38 https://www.bbc.co.uk/news/world-middle-east-68478828#:~:text=Several%20undersea%20communications%20cables%20in,15%20cables%20were%20recently%20severed; https://www.ft.com/content/bf17fc55-8624-435b-b7dd-bc662a887ba0

39 https://www.internetsociety.org/resources/doc/2024/2024-west-africa-submarine-cable-outage-report/#:~:text=On%2014%20March%202024%2C%20a,3%2FWest%20Africa%20Submarine%20Cable

40 https://cto.int/about-the-cto/news-and-media/cto-newsletter/tonga-restores-international-connectivity-after-five-week-outage/#:~:text=The%20international%20submarine%20cable%20that,weeks%20to%20repair%20the%20damage.

41 https://unidir.org/publication/wading-murky-waters-subsea-communications-cables-and-responsible-state-behaviour/

42 https://www.gov.uk/government/news/new-undersea-capability-to-strengthen-aukus-partnership; https://www.forces.net/services/navy/royal-navy-task-force-deploys-defend-critical-undersea-data-cables

43 https://www.nato.int/cps/en/natohq/news_219441.htm

44 https://www.gov.uk/government/news/royal-navy-infrastructure-protection-ship-accelerated, https://www.royalnavy.mod.uk/news-and-latest-activity/news/2023/october/10/20231010-uk-protection-enhanced-as-underwater-surveillance-ship-enters-service

45 https://www.institute.global/insights/geopolitics-and-security/software-and-hard-war-building-intelligent-power-artificially-intelligent-warfare

46 https://www.nato.int/cps/en/natohq/topics%5F175419.htm

47 https://www.armscontrol.org/act/2024-03/news/us-warns-new-russian-asat-program

48 https://fas.org/publication/russia-space-nuclear-weapons/

49 https://www.theguardian.com/world/2024/feb/29/north-korea-spy-satellite-malligyong-1-alive-running-in-use

50 https://www.reuters.com/technology/space/irans-pars-1-satellite-enters-space-after-russian-launch-2024-02-29/

51 https://www.defensenews.com/digital-show-dailies/dsei/2021/09/14/head-of-uks-space-directorate-warns-of-space-terrorism/

52 https://www.spoc.spaceforce.mil/Portals/4/Images/2%5FSpace%5FSlicky%5F11x17%5FWeb%5FView%5Freduced.pdf, https://www.bloomberg.com/news/articles/2024-01-25/china-russia-disguise-threats-posed-by-satellites-us-space-force-says

53 https://www.bbc.co.uk/news/articles/cne900k4wvjo#:~:text=Russia%20is%20causing%20disruption%20to,Global%20Positioning%20System%20%28GPS%29.

54 https://www.gpsworld.com/chinas-beidou-challenges-u-s-gps-dominance/

55 https://spacenews.com/eutelsat-scales-back-oneweb-gen-2-upgrade-plan/#:~:text=UK%20pushing%20to%20combine%20OneWeb,merged%20with%20Eutelsat%20of%20France. https://spacenews.com/uk-pushing-to-combine-oneweb-gen-2-and-european-sovereign-constellation-efforts/

56 https://www.theengineer.co.uk/content/in-depth/zephyr-high-altitude-solar-powered-aircraft-gears-up-for-commercial-service/

57 https://www.institute.global/insights/politics-and-governance/a-new-national-purpose-leading-the-biotech-revolution

58 https://www.ginkgobioworks.com/offerings/biosecurity-services/

59 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf

60 https://www.gov.uk/government/news/uk-japan-and-italy-sign-international-stealth-fighter-jet-programme-treaty

61 https://hansard.parliament.uk/lords/2023-12-19/debates/8C98D00A-7736-4FEF-B93F-C0AD5B85DDEE/GlobalCombatAirProgrammeTreaty

62 https://www.theguardian.com/australia-news/2023/apr/05/future-undersea-warfare-will-rely-on-uncrewed-submarines-as-ocean-becomes-transparent-defence-contractor-says, https://breakingdefense.com/2024/04/andurils-aussie-drone-sub-one-year-early-and-on-budget-heads-to-production/

63 https://foreignpolicy.com/2024/04/06/us-army-military-robots-soldiers-technology-testing-war/

64 https://www.gov.uk/government/news/un-jammable-quantum-tech-takes-flight-to-boost-uks-resilience-against-hostile-actors

65 https://assets.publishing.service.gov.uk/media/6411a602e90e0776996a4ade/national%5Fquantum%5Fstrategy.pdf

66 https://www.reuters.com/technology/japans-fujitsu-riken-develop-second-quantum-computer-2023-10-05/

67 https://commonslibrary.parliament.uk/research-briefings/cbp-9842/

68 https://committees.parliament.uk/committee/127/public-accounts-committee/news/200289/uk-defence-no-credible-government-plan-to-deliver-desired-military-capabilities/

69 https://www.ipsos.com/en-uk/four-in-ten-support-plans-to-increase-defence-spending#:~:text=The%20poll%20found%20that%2042,in%20support%20and%2034%25%20opposed.

70 https://breakingdefense.com/2021/11/un-committee-votes-yes-on-uk-us-backed-space-rules-group/, https://www.espi.or.at/reports/whats-next-for-europe-in-multilateral-engagement-on-space-security/, https://breakingdefense.com/2023/09/russia-spikes-un-effort-on-norms-to-reduce-space-threats/

71 https://assets.publishing.service.gov.uk/media/6620cf9a77a30aa0c4757d35/rhc%5Freport%5Fon%5Fthe%5Ffuture%5Fregulation%5Fof%5Fspace%5Ftechnologies.pdf

72 https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/

73 https://publications.parliament.uk/pa/ld5804/ldselect/ldaiwe/16/16.pdf https://ccdcoe.org/uploads/2020/02/UN-191213%5FCCW-MSP-Final-report-Annex-III%5FGuiding-Principles-affirmed-by-GGE.pdf

74 https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2022/gge/documents/UK_March2022.pdf

75 https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf

76 https://assets.publishing.service.gov.uk/media/65e07110cf7eb16adff57ff4/Integrated%5FProcurement%5FModel.pdf

77 https://www.defense.gov/Spotlights/AUKUS/

78 https://committees.parliament.uk/writtenevidence/127745/pdf/

79 https://cset.georgetown.edu/article/the-future-of-drones-in-ukraine-a-report-from-the-diu-brave1-warsaw-conference/

80 https://www.cr14.ee/

81 https://www.kyivpost.com/post/30149

82 https://defensescoop.com/2023/02/01/deploying-contractor-owned-robotic-vessels-could-be-a-fruitful-long-term-option-for-the-navy-secretary-del-toro-says/

83 https://www.route-fifty.com/digital-government/2020/10/how-the-armys-dora-bot-cuts-manual-work-for-contracting-professionals/315706/

84 https://www.gov.uk/government/organisations/defence-and-security-accelerator

85 https://www.gov.uk/government/organisations/jhub-defence-innovation

86 https://www.gov.uk/government/publications/dasa-annual-review-2022-23#:~:text=DASA%20is%20pleased%20to%20publish,of%20DASA's%20work%20with%20suppliers

87 https://ww2.aip.org/fyi/2023/fy23-budget-outcomes-department-defense#:~:text=DARPA.,Defense%20Innovation%20Unit

88 https://rusi.org/explore-our-research/publications/commentary/joint-expeditionary-force-digital-better-way-deliver-defence-tech

89 https://committees.parliament.uk/writtenevidence/122267/pdf/

90 https://committees.parliament.uk/writtenevidence/125575/html/

91 https://www.defense.gov/News/Releases/Release/Article/3403601/dod-announces-second-set-of-projects-to-receive-funding-from-the-pilot-program/

92 https://www.defense.gov/News/Releases/Release/Article/3543777/department-of-defense-and-small-business-administration-roll-out-the-small-busi/

93 https://pitchbook.com/news/articles/defense-space-vc-ukraine-recession

94 https://www.ft.com/content/18e62451-d066-497e-93dd-f42decd59410; https://www.rusi.org/explore-our-research/publications/commentary/joint-expeditionary-force-fund-better-way-finance-defence; https://www.americanprogress.org/article/natos-financing-gap/; https://tradingeconomics.com/country-list/rating

95 https://www.rusi.org/explore-our-research/publications/commentary/joint-expeditionary-force-fund-better-way-finance-defence

96 https://www.defensenews.com/industry/2023/07/11/bae-systems-wins-order-for-munitions-as-uk-rebuilds-stocks/

97 https://www.politico.com/news/2023/12/19/missile-drone-pentagon-houthi-attacks-iran-00132480

98 https://www.nato.int/cps/en/natohq/topics%5F222589.htm#:~:text=At%20the%202023%20Vilnius%20Summit,capacity%20and%20enhance%20Allies'%20interoperability.

99 https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-has-a-new-plan-to-ramp-up-defense-production-is-it-enough/

100 https://edition.cnn.com/2024/03/10/politics/russia-artillery-shell-production-us-europe-ukraine/index.html

101 https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-01/230119%5FJones%5FEmpty%5FBins.pdf

102 https://www.theguardian.com/world/2024/mar/19/czech-republic-to-deliver-thousands-of-extra-artillery-shells-to-ukraine

103 https://committees.parliament.uk/publications/43178/documents/214880/default/

104 https://www.gov.uk/government/news/pm-announces-turning-point-in-european-security-as-uk-set-to-increase-defence-spending-to-25-by-2030

105 https://www.army-technology.com/analyst-comment/reviewing-uk-defence-supply-chain/?cf-view

106 https://www.rand.org/pubs/research%5Freports/RRA1739-1.html

107 https://www.c4isrnet.com/battlefield-tech/space/2022/05/02/how-the-space-force-is-working-with-us-allies/

108 https://defensescoop.com/2024/03/11/replicator-funding-2024-2025-hicks/

109 https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-has-a-new-plan-to-ramp-up-defense-production-is-it-enough/

110 https://cepa.org/comprehensive-reports/elevating-our-edge-a-path-to-integrating-emerging-and-disruptive-technologies/

111 https://www.army.mod.uk/media/11826/20210322-army-future%5Fsoldier-publication-final.pdf

112 https://researchbriefings.files.parliament.uk/documents/CBP-7930/CBP-7930.pdf

113 https://assets.publishing.service.gov.uk/media/648ad6b8b32b9e000ca967c9/Incentivising%5Fpeople%5Fin%5Fa%5Fnew%5Fera%5F-%5Fa%5Freview%5Fof%5FUK%5FArmed%5FForces.pdf

114 https://committees.parliament.uk/writtenevidence/127745/pdf/

115 https://www.stemwomen.com/women-in-stem-statistics-progress-and-challenges

116 https://www.gov.uk/government/statistics/uk-armed-forces-biannual-diversity-statistics-october-2023

117 https://www.foreignaffairs.com/united-states/ai-already-war-flournoy

118 https://www.gov.uk/government/news/new-50-million-cyber-academy-to-benefit-influential-uk-us-relationship

119 https://creative.bfbs.com/genz

120 https://yougov.co.uk/politics/articles/45896-what-do-public-think-should-happen-armed-forces

121 https://committees.parliament.uk/publications/6959/documents/72771/default/; https://committees.parliament.uk/oralevidence/13817/pdf/

122 https://assets.publishing.service.gov.uk/media/648ad6b8b32b9e000ca967c9/Incentivising%5Fpeople%5Fin%5Fa%5Fnew%5Fera%5F-%5Fa%5Freview%5Fof%5FUK%5FArmed%5FForces.pdf

123 https://assets.publishing.service.gov.uk/media/5f324f7ad3bf7f1b1ea28dca/SECONDARY%5Fnational%5Fcurriculum%5F-%5FCitizenship.pdf

124 https://labour.org.uk/wp-content/uploads/2022/10/WR-16813%5F22-Labour-Skills-Council-report-Edit-19-10-22.pdf

125 https://www.foreignaffairs.com/united-states/ai-already-war-flournoy

126 https://www.shift.org/dv; https://warontherocks.com/2024/03/american-military-civil-fusion-at-risk-with-the-loss-of-the-shift-fellowship/

127 https://commonslibrary.parliament.uk/research-briefings/cbp-7930/#:~:text=On%201%20April%202023%20the,Royal%20Air%20Force%20%28RAF%29

128 https://www.thetimes.co.uk/article/uk-military-is-too-small-to-fight-key-allies-warn-f6lv9gtxw

129 https://researchbriefings.files.parliament.uk/documents/CBP-7930/CBP-7930.pdf

130 https://committees.parliament.uk/writtenevidence/128129/default/

131 https://committees.parliament.uk/oralevidence/14154/pdf/

132 https://committees.parliament.uk/writtenevidence/128129/default/, https://committees.parliament.uk/oralevidence/14154/pdf/

133 https://www.thetimes.co.uk/article/army-applicants-give-up-after-waiting-six-months-to-join-dn2vtbfdd

134 https://committees.parliament.uk/oralevidence/14154/pdf/

135 https://www.thetimes.co.uk/article/hundreds-of-soldiers-moved-to-recruitment-offices-zscp60vjq

136 https://www.thetimes.co.uk/article/put-soldiers-back-in-charge-of-recruiting-tkmgw29kw

137 https://www.gov.uk/government/news/shaping-the-future-of-defence-recruitment

138 https://www.telegraph.co.uk/news/2024/01/27/military-staffing-crisis-deepens-recruitment-scheme-delayed/; https://questions-statements.parliament.uk/written-questions/detail/2023-12-18/7263

139 Accessible tables to UK armed forces quarterly service personnel statistics: 1 January 2024, Table 4 https://www.gov.uk/government/statistics/quarterly-service-personnel-statistics-2024

140 Accessible tables to UK armed forces quarterly service personnel statistics: 1 January 2024, Table 5d https://www.gov.uk/government/statistics/quarterly-service-personnel-statistics-2024

141 https://assets.publishing.service.gov.uk/media/648ad6b8b32b9e000ca967c9/Incentivising_people_in_a_new_era_-_a_review_of_UK_Armed_Forces.pdf

142 https://www.gov.uk/government/groups/joint-cyber-reserve-force

143 https://www.thetimes.co.uk/article/882348dd-f48f-4c46-af94-0a9ea8a4fcee?shareToken=17ec9aadb601b991c0ef171fd5a59da2

144 https://www.foreignaffairs.com/united-states/ai-already-war-flournoy

145 https://assets.publishing.service.gov.uk/media/64b55dd30ea2cb000d15e3fe/Defence%5FCommand%5FPaper%5F2023%5FDefence%5Fs%5Fresponse%5Fto%5Fa%5Fmore%5Fcontested%5Fand%5Fvolatile%5Fworld.pdf

146 https://news.sky.com/story/uk-risks-being-unable-to-call-up-vital-personnel-without-national-plan-for-war-says-military-analyst-13107252#:~:text=In%20the%20event%20of%20a,positions%20in%20the%20country's%20defences.

147 https://www.ncsc.gov.uk/section/industry-100/about; https://www.ncsc.gov.uk/blog-post/five-years-of-i100

148 https://data.parliament.uk/DepositedPapers/Files/DEP2022-0997/6.8213%5FCO%5FResilience%5FFramework%5FFINAL1.pdf

149 https://www.thetimes.co.uk/article/sweden-shows-us-the-way-to-defend-our-infrastructure-7wxfb58gn, https://www.msb.se/en/training--exercises/

150 https://news.sky.com/story/govt-has-no-national-plan-for-defence-of-the-uk-in-a-war-despite-renewed-threats-of-conflict-13106616

151 https://www.telegraph.co.uk/news/2024/04/06/britain-is-not-ready-for-war-ministers-defence-mod/

152 https://news.sky.com/story/govt-has-no-national-plan-for-defence-of-the-uk-in-a-war-despite-renewed-threats-of-conflict-13106616, https://www.theguardian.com/uk/2009/jun/23/britain-nuclear-war-plans-published

153 https://www.gov.uk/government/speeches/deputy-prime-minister-annual-resilience-statement; https://prepare.campaign.gov.uk/

154 https://warontherocks.com/2024/04/in-from-the-cold-rebuilding-swedens-civil-defense-for-the-nato-era/; https://rib.msb.se/filer/pdf/30307.pdf

155 https://www.cityam.com/nato-needs-enhanced-capabilities-not-just-more-funding/

156 https://www.reuters.com/world/us-reduce-licensing-by-80-uk-australia-boost-aukus-2024-04-18/

157 https://www.gov.uk/government/news/aukus-partnership-to-consult-with-other-nations-including-japan-on-military-capability-collaboration; https://www.reuters.com/world/south-korea-confirms-talks-aukus-pact-with-us-uk-australia-2024-05-01/; https://www.telegraph.co.uk/world-news/2024/04/08/canada-justin-trudeau/

158 https://www.rusi.org/explore-our-research/publications/commentary/stretching-joint-expeditionary-force-idea-our-times

159 https://commonslibrary.parliament.uk/research-briefings/cbp-8175/

160 https://www.gov.uk/government/statistics/mod-trade-industry-and-contracts-2023/mod-trade-industry-and-contracts-2023

161 https://www.rand.org/pubs/research%5Freports/RRA1739-1.html

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

facebook.com/instituteglobal
twitter.com/instituteGC
instagram.com/institutegc

General enquiries

info@institute.global