House of Lords
House of Commons

Joint Committee on the National Security Strategy

The National Security Strategy: Government Response

First Special Report of Session 2026–27

HC 337
HL Paper 20

Joint Committee on the National Security Strategy

The Joint Committee on the National Security Strategy is appointed by the House of Lords and the House of Commons to consider the National Security Strategy.

Current membership

House of Lords

Lord Arbuthnot of Edrom (Conservative; Life peer)

Lord Boateng (Labour; Life peer)

Lord Godson (Conservative; Life peer)

Lord Hutton of Furness (Labour; Life peer)

Lord Jack of Courance (Conservative; Life peer)

Baroness Kidron (Crossbench; Life peer)

Lord Sedwill (Crossbench; Life peer)

Lord Tunnicliffe (Labour; Life peer)

Baroness Tyler of Enfield (Liberal Democrat; Life peer)

Lord Watts (Labour; Life peer)

House of Commons

Matt Western (Labour; Warwick and Leamington) (Chair)

Dame Karen Bradley (Conservative; Staffordshire Moorlands)

Liam Byrne (Labour; Birmingham Hodge Hill and Solihull North)

Sarah Champion (Labour; Rotherham)

Mr Tanmanjeet Singh Dhesi (Labour; Slough)

Bill Esterson (Labour; Sefton Central)

Mike Martin (Liberal Democrat; Tunbridge Wells)

Edward Morello (Liberal Democrat; West Dorset)

Andy Slaughter (Labour; Hammersmith and Chiswick)

Emily Thornberry (Labour; Islington South and Finsbury)

Derek Twigg (Labour; Widnes and Halewood)

Sir Gavin Williamson (Conservative; Stone, Great Wyrley and Penkridge)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place within the United Kingdom, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chair.

Publication

This Report was Ordered by the House of Commons, on 15 June 2026, to be printed. It was published on 24 June 2026 by authority of the House of Commons.

Committee Reports are published on the Committee's website at www.parliament.uk/jcnss and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on the National Security Strategy, House of Commons, London SW1A 0AA. The Committee's email address is jcnss@parliament.uk.

Follow the work of committees on Bluesky @HOCcommittees.parliament.uk, Facebook UK House of Commons Committees, Instagram @UKCommonsCommittees, LinkedIn House of Commons Committees, Reddit u/UKCommonsCommittees, X @HOCcommitteesUK and YouTube Commons Committees playlist.

First Special Report

The Committee published its Fourth Report of Session 2024–26, The National Security Strategy (HC 1045, HL Paper 281), on 27 March 2026. The Government's response was received on 1 June 2026 and is appended to this report.

Appendix: Government response

The Government is grateful to the Joint Committee on the National Security Strategy for their inquiry into the National Security Strategy published in June 2025. The report suggests there are gaps in the Government's plans for delivery, funding, and oversight while acknowledging the radical uncertainty of the current global security environment. The Government agrees with many of the recommendations and has outlined work being undertaken to address the Committee's concerns.

The response to the Committee's recommendations is below:

Engagement with Stakeholders

Conclusion: The Government must balance transparency with the public about the reality of threats the UK faces with not causing alarm and making sensitive information unnecessarily accessible to adversaries. However, there is a sense among industry stakeholders and civil society organisations that they were not sufficiently consulted in the development of the National Security Strategy, and a subsequent lack of transparency on certain important aspects such as the China Audit and timelines. The lack of publicly available detail, particularly around the issue of China, risks eroding public trust that progress is being made to improve national security. The lack of engagement with stakeholders makes securing the buy-in needed for a whole-of-society approach to resilience more challenging. (Paragraph 21).

Recommendation: The Government must reconsider how it discusses security challenges, and avoid being unduly opaque. The Government should provide annual progress updates to this Committee on commitments in the National Security Strategy and in other related strategies such as the Resilience Action Plan. The first of these updates should be provided alongside the Government's response to this report."(Paragraph 22).

Recommendation: The Government should also review its consultation and engagement approach with industry stakeholders, civil society and the wider public on matters of national security. (Paragraph 23).

The Government agrees on the importance of building public awareness of the threats we face and engaging with industry on working to mitigate those. In developing the National Security Strategy, the Government engaged a broad spectrum of stakeholders, considered assessments and analytical products from think tanks, academics, industry experts and reports from the Intelligence and Security Committee and the Joint Committee on the National Security Strategy (JCNSS). It also brought together several strategies, reviews, and audits developed and being developed by the government. These reviews had their own method of engagement, including with civil society organisations and industry. This includes the Resilience Action Plan which a large number of stakeholders, including civil society organisations, were engaged with to support development and delivery.

The then Foreign Secretary fulfilled his commitment to update the House on the China Audit. We carried out a comprehensive audit on the breadth of the UK's relationship with China, which is informing a consistent, long-term and strategic approach, rooted in UK and global interests. This 'Audit' informed the National Security Strategy, the Strategic Defence Review and our Trade and Industrial Strategies.

The Resilience Action Plan outlines our ambition for resilience to be a whole-of-society effort. Since its publication we have run a public consultation on how to strengthen partnerships between categorised emergency responders and the voluntary, community and faith sector organisations, and we have established a programme of engagement with critical stakeholders and civil society organisations. In July 2025 we published insights from the first UK Public Survey of Risk Perception, Resilience and Preparedness, and we plan to publish findings from the 2026 survey later this year, demonstrating our commitment to engaging with the public on matters of resilience.

The UK is committed to driving a whole-of-society approach through its world-leading "transparent by default approach". HMG is committed to shifting the culture of resilience and the way threats are considered in

the UK. The National Risk Register (NRR) is our public facing articulation of the risks facing us, with the last update published in January 2025. A "transparent by default" approach has been adopted, declassifying and sharing information from the internal version, the National Security Risk Assessment (NSRA), except in a small number of highly sensitive areas. In July 2025 we published insights from the first UK Public Survey of Risk Perception, Resilience and Preparedness, released as Official Statistics in Development. We plan to publish findings from the 2026 survey later this year, demonstrating our commitment to monitor trends and evaluate the impact of public communications on preparedness. We will continue to make an annual statement to Parliament on resilience, as set out in our Resilience Action Plan.

This government has also published its Defence Industrial Strategy, which outlines our new approach, not just to defence procurement, but also how we engage with industry throughout the supply chain. The upcoming Defence Readiness Bill will improve how we work collectively with industry to improve the readiness of our defence sector.

Soft power, development and national security

Conclusion: Soft power is a crucial source of UK influence and security abroad. Its erosion would have direct security consequences, most clearly in Africa, where Russia and China are increasingly filling the space left by the withdrawal of the soft power presence of the UK and allies. Official Development Assistance and bodies such as the BBC World Service and the British Council play an important role in regions where the UK has clear security interests. The recent funding commitments to the BBC World Service are welcome in this regard. (Paragraph 32).

Recommendation: The Government should ensure it has a full and robust assessment of the national security risks of reducing the Official Development Assistance budget, resisting further cuts that could have a damaging effect for UK strategic interests. We note the International Development Committee is further examining the future of UK aid and hope the Government will engage with that inquiry constructively. The Government should ensure stable and predictable funding for bodies such as the BBC World Service and British Council, and draw on the advice of experts represented on the Soft Power Council. The next iteration of the National Risk Register should account for the possible impacts of reducing UK and allied soft power. (Paragraph 33).

The Government agrees that soft power is a vital source of UK influence and security, particularly in regions facing growing instability and strategic competition. That is why the Government has established the UK Soft Power Council, made up of leaders from the UK's soft power and international policy sectors.

The UK's bilateral relationships with key partners are broader than simply how much aid we spend, which is why the UK is transforming our country's development partnerships, reflecting the changing needs of our partners as part of our development reset.

Official Development Assistance remains an important part of our broad soft power toolkit, alongside diplomacy, defence and trade. That is why, even while taking difficult decisions to reduce the aid budget in order to increase defence spending in a more dangerous world, we are protecting the effectiveness of our development offer and modernising how we deliver it.

Our ODA is increasingly focused on fragile and conflict-affected states, where instability can be exploited by malign actors and where development, humanitarian action and security are most closely linked. We are also backing institutions that project UK values and reach at scale. In that context, the Government's increased grant funding for the BBC World Service and the British Council demonstrates our firm commitment to trusted media, cultural, and educational links.

The Government recognises the importance of understanding the national security implications of changes to the Official Development Assistance budget. Decisions to reduce ODA were taken in the context of the most serious security pressures in a generation, but they were not taken lightly. That is why we have changed our approach to focus ODA more sharply on fragile and conflict-affected contexts and on interventions that support long-term stability, resilience and conflict prevention.

We welcome scrutiny of the UK's development approach and are engaging constructively with the International Development Committee's inquiry. Transparency, predictability and value for money are central to the new three-year ODA settlements, which provide greater funding certainty than in recent years.

The Government also agrees on the importance of stable grant funding for key soft power institutions, while noting that government grants are not the primary source of funds for either the BBC World Service or the British Council. The Government is continuing to draw on the advice and expertise of the UK Soft Power Council. As part of a whole-of-government approach to risk, we shall continue to ensure that assessments of national resilience and international risk take account of the role of UK soft power.

Conclusion: The lack of clarity over which departments are responsible for which areas of national security policy hampers the possibility for external scrutiny and challenge of national security policy delivery. Our opinion was further solidified when the Department for Science, Innovation and Technology declined to put forward a minister to give evidence to this inquiry alongside the Chancellor of the Duchy of Lancaster and the Minister for Security. (Paragraph 40).

Recommendation: The Government must clarify how follow-up and oversight of Lead Government Departments responsible for delivering the commitments in the National Security Strategy (NSS) will be sustained over time. This should involve accountability mechanisms at fixed points, for example through regular reporting to the National Security Adviser and his Deputies. These reporting updates should be included in the regular updates to the Committee, called for in an earlier recommendation. The Government should also publish an addendum to the NSS, which assigns delivery responsibilities for the commitments made in the Strategy to named Ministers within each department. (Paragraph 41).

Recommendation: All Ministers with responsibility for delivery of aspects of the National Security Strategy should make themselves available for scrutiny by this Committee at regular intervals, and as requested, to ensure proper parliamentary accountability. (Paragraph 42).

The Government has developed an internal implementation approach to ensure accountability and delivery of the National Security Strategy objectives. Our national security is not the remit of one department or minister; we have identified specific objectives and assigned lead and assisting departments. They are responsible for periodic reporting on progress and taking action to address any deficiencies. The Government has offered to update the Committee on progress through formal public sessions and confidential sessions where appropriate.

The Government supports the principle of Ministerial accountability and Ministers should attend sessions when called upon. However, the Government should be able to confirm which Ministers are best placed to represent the issue at hand and can best provide the Committee the Government's position.

Funding

Conclusion: Hitting the target to spend 1.5% of GDP on resilience and security by 2027 will be a limited achievement if it does not create any additional resilience capability for the UK beyond what was already allocated in the 2025 Spending Review. We appreciate that the 1.5% target is still new, but a long-term lack of clarity over what will be included within the target creates uncertainty for private and public bodies involved in resilience planning. (Paragraph 46).

Recommendation: The Government must provide greater clarity on its plans to develop additional resilience capabilities beyond 2027, and ensure that the 1.5% target spend on security and resilience prioritises investment in systems that can help build long-term resilience, in addition to spending on maintenance of basic civil infrastructure. The Government should also clearly outline what additional capabilities it envisages developing through the target spend by the time of the next NATO summit in July 2026. (Paragraph 47).

NATO has already agreed the definition of 1.5% as spending to protect critical infrastructure, defend networks, ensure civil preparedness and resilience, innovate, and strengthen the defence industrial base.

We have long argued that investment in areas like energy security is vital to national security. That is reflected in our National Security Strategy, Resilience Action Plan and in our Spending Review settlement and we are pleased it is now recognised by NATO.

We expect we will reach the 1.5% target by 2027 and will report our spending lines to NATO shortly. As with many national security capabilities we would expect this to be a combination of both capital and non-capital spending.

Protecting Critical National Infrastructure

Conclusion: We welcome the greater use of Armed Forces Reserves in protecting Critical National Infrastructure (CNI), but necessary detail on these plans is lacking. Private sector organisations with responsibility for the protection of CNI also need a clearer steer on what they will be expected to do to bolster resilience of CNI, including in cyber-resilience. (Paragraph 57).

Recommendation: The Government must accelerate its plans for improving the size and state of the reserves, and provide more detail for its plans to involve the reserves in the protection of Critical National Infrastructure. This should include planning for their use to replace uniformed specialists who have been moved to frontline services;

the continued functioning of services in a communications and supplies-degraded environment; and plans for deployment in a crisis. (Paragraph 58).

Recommendation: The Government should clarify what will change for private sector Critical National Infrastructure operators as a result of the NSS and provisions of the Cyber Security and Resilience (Network and Information Systems) Bill. It should then work with those operators to identify what support will be needed for them to adapt to the new regime. (Paragraph 59).

The Government is committed to working closely with owners and operators of CNI in the UK to maintain and improve the cyber resilience of our most critical systems. Critical National Infrastructure (CNI) Lead Government Departments are responsible for setting the guidance and expectations that support their sectors' resilience efforts. The Cabinet Office has committed to mapping these resilience standards, which are fundamental in holding industry to account and assuring the resilience of UK CNI. This mapping will be used to identify and address any gaps in the steer provided to CNI owners and operators regarding their resilience activities across all risks, including for cyber. Additionally, the National Protective Security Authority (NPSA) is working on developing guidance to support CNI (and wider Industry) to better understand what is expected in terms of protective security at their locations.

As part of the Armed Forces Bill 2026, we are amending the Reserve Forces Act (RFA 96), which makes provision for matters including call-out for and recall to permanent service. These measures will help us respond to the unstable geopolitical outlook and latest threats that we face.

In response to Strategic Defence Review Recommendation 27, and as part of wider government plans to improve the protection of CNI, the Ministry of Defence is exploring the development of a new force that is modelled on the Reserves. We will provide further public details in due course. This is part of HMG's wider work to raise CNI resilience across the UK, as set out in the Resilience Action Plan, including work by Government with industry and National Technical Authorities to identify and prioritise where targeted interventions are required.

This includes through the Cyber Security and Resilience Bill, which covers operators of essential services in the energy, transport, health, drinking water sectors, data and digital infrastructure and some digital services. The Bill requires in-scope organisations to meet proportionate cyber security and resilience requirements, consistent with the NCSC's Cyber Assessment Framework and regulator guidance. They must also report more harmful incidents to their regulator and notify the NCSC within 24 hours, with a full report due within 72 hours.

The Government will support organisations in meeting the Bill's requirements through various methods, including implementation guidance for regulators, who themselves produce sector-specific compliance guidance. The Secretary of State will also have the power to issue a code of practice, which will clarify expectations and aid compliance for regulators and businesses.

There is also a wide range of guidance, tools, training and support provided by the Government to support organisations to drive up cyber maturity. This includes the Cyber Governance Code of Practice to help organisations manage cyber risks, the Cyber Essentials scheme to prevent common cyber attacks (including in their supply chains) and the use of the Early Warning service.

The upcoming National Cyber Action Plan will outline further concrete actions to strengthen our resilience and harness cyber's enormous growth opportunities, including for CNI.

Scrutiny of public sector resilience

Conclusion: While we welcome ambitions to scrutinise resilience plans through the UK Resilience Academy, it is unclear at this stage how effective its scrutiny will be. How far its scrutiny remit will stretch, and whether this will include reviewing preparedness plans in the event of a crisis or warfighting situation, and/or increasingly sophisticated attacks facilitated through novel technologies, are all outstanding questions. (Paragraph 66).

Recommendation: The Government should ensure that the UK Resilience Academy is reviewing preparedness plans specifically in relation to the estimated impacts of Reasonable Worst Case Scenarios as set out in the National Risk Register, including the possibility of direct threat to the homeland. (Paragraph 67).

Recommendation: The Government should also set out, in response to this report, how it will strengthen institutional links between the UK Resilience Academy (UKRA) and central government, including by: enabling the UKRA to report into Cabinet Office-led exercises to refresh the National Risk Register to inform impact and preparedness estimates; reporting into the National Exercising Programme; and ensuring there is always UKRA representation in these exercises. (Paragraph 68).

The Government agrees with both recommendations. The UK government will maintain responsibility for the delivery of our response plans and preparations. The UK Resilience Academy (UKRA) is committed to enhancing the provision of independent advice and challenge to the UK government,

and will incorporate perspectives of the UK's leading experts on various complex risks into our work. It is being instructed to convene a number of panels per year composed of relevant experts to scrutinise plans and preparedness for whole-system civil emergencies across the UK. They will scrutinise our planning via document reviews and interviews with key officials and offer recommendations on improvements that can be made to the Cabinet Office as well as to the Lead Government Department for the specific risk they are considering.

The UKRA is a key partner of the National Exercising Programme, and is currently playing a significant role in developing a national exercising hub, which will host, among other things an exercising tracker for Tier 1 and 2 exercises, comprehensive guidance on exercising best practice and doctrine and how we work with NSRA/NRR colleagues to link exercising with risk monitoring and mitigation.

Public awareness and whole-of-society approach

Conclusion: The Government has identified the need for a whole-of-society approach to security and resilience through a national conversation, but it is not evident that this message is getting through to the public. There is a long way to go to realise the whole-of-society approach to defence and security. (Paragraph 74).

Recommendation: The Government must provide more detail on what the national conversation on security and resilience will look like, including who will be leading it and how it will ensure oversight between different Government departments responsible for its delivery. As part of this, the Ministry of Defence should publish the public version of its Joint Concept Note as soon as possible. (Paragraph 75).

Through the Resilience Action Plan, we have committed to communicating the actions recommended for individuals, households, communities and businesses to increase their own preparedness and resilience, as set out on GOV.UK/Prepare. And through the Strategic Defence Review, we commit to a national conversation to raise public awareness of the threats to the UK, what we are doing to deter and protect against them, and why Defence requires support to strengthen the nation's resilience.

The national conversation on security and resilience is a Government-wide effort. As the Prime Minister confirmed in March, it is already underway: over the last few months the Minister for the Armed Forces, the Director General of MI5, the Chief of the Defence Staff, the Defence Secretary and the Prime Minister have all spoken directly on the threats we face and what we are doing to deter and protect against them.

In July 2025 we published insights from the first UK Public Survey of Risk Perception, Resilience and Preparedness, and we plan to publish findings from the 2026 survey later this year, demonstrating our commitment to understanding trends and adapting our thinking as we build a whole-of-society approach to security and resilience. We remain committed to raising the public's awareness of the risks and threats we face, and sharing information that will help the public better prepare for emergencies, be more informed about hazards, and get involved in activities that support their community before, during and after an emergency.

We will publish updated or new publicly accessible information, including the Joint Concept Note, in due course.

Pillar 2 - Strength Abroad - overview

Conclusion: Global and UK security is poorly served by the increasing tensions brought about by great power competition between the United States and China. If this process continues to accelerate, the economic shock costs of military confrontation will go down, making conflict more likely. The post-war security settlement has served the UK, Europe and the world well for over 80 years, and while the UK's influence is less than it once was, there is still an imperative to do what it can to maintain and bolster these arrangements. (Paragraph 79).

Recommendation: The UK must be prepared to take on more of the cost for its and Europe's security through investing in partnerships and multilateral dialogues with other 'middle powers', for example Canada, Australia and India, to avoid being squeezed by great power competition between the United States and China. UK long-term strategy should seek to ease the increasing tensions of great power competition between the United States and China, and the global diplomatic and economic decoupling this is resulting in. In turn, this will bolster both UK and global security. (Paragraph 80).

The Government agrees with the recommendation. This largely summarises what is set out in the strategy. The National Security Strategy 2025 acknowledges that the international order is undergoing radical uncertainty, driven by intensified great power competition, authoritarian aggression, and extremist ideologies. Many of the established rules of the international system are eroding. Consequently, our statecraft must adapt to a more competitive and transactional global environment, particularly concerning migration, defence, energy, technology, and raw materials.

The threat from Russia

Conclusion: The Government has identified Russia as the primary threat to the UK's national security and continues to do good work to deter further Russian aggression. The Committee commends the Government for its continued military and financial assistance for Ukraine and its planned investment in sharpening the UK's hard power, including through maintenance of the independent nuclear deterrent. In conjunction with NATO allies, the UK also continues to demonstrate a united front against Russian aggression by tightening the pressure on Moscow through use of sanctions and acting against the shadow fleet. (Paragraph 88).

Recommendation: As long as Russia continues its war in Ukraine, and acts of hybrid aggression against the UK and its European allies, the Government must ensure that momentum in imposing ever greater costs on Russia is maintained. The UK must continue to take a leadership role in this within European NATO. With this in mind, the Government should hasten publication and progress of strategies, legislation and reviews relevant to the hardening and sharpening of the UK's conventional, hybrid and cyber capabilities, including the Defence Investment Plan, the Defence Readiness Bill and the Rycroft Review. The Government should also set out its priorities in the Arctic and the High North in the response to this report, and engage fully and constructively with the Defence Committee's inquiry in this area. (Paragraph 89).

We welcome the support from the Committee on the Government's work to counter the threat from Russia and ensure Ukraine is supported militarily and financially in its defence against Russia's illegal invasion. The Government will continue to work with NATO Allies to counter Russian aggression, as well as through other groupings in Europe as Europe continues to step up on defence, such as with the Joint Expeditionary Force where the UK is Framework Nation.

The Government also agrees with the importance of the UK continuing to take a leadership role in a more European NATO. The Prime Minister set out his vision for this in his speech at the Munich Security Conference in February, where he noted the threat from Russia and the need for a stronger Europe and a more European NATO, underpinned by deeper links between the UK and the EU, across defence, industry, tech, politics, and the wider economy. The Arctic and High North is a significant priority for the government as part of this work and the UK is participating in NATO's Arctic Sentry activity that is strengthening NATO's posture in the Arctic and High North.

The Defence Investment Plan (DIP) will be published shortly. The Defence Readiness Bill should provide the Government with powers in reserve to mobilise the Reserves and industry, should a crisis escalate into conflict. It should also facilitate external scrutiny of UK warfighting readiness.

The Government will respond in full to the Rycroft's report findings within the coming months, but we are already taking immediate steps to implement his recommendations for a cap on donations made by overseas electors and for a moratorium on donations made via cryptocurrency, which we will implement through the Representation of the People Bill.

The threat from China

Conclusion: China poses a clear long-term national security threat to the UK—both directly through its malicious targeting of UK interests, and indirectly through its support to Russia over the Ukraine conflict. We have concerns that the Government is not striking the right balance—and indeed about whether it is prepared to accept the unpalatable reality that long-term security has short-term financial costs. (Paragraph 104).

Recommendation: The Government must articulate more clearly how it will balance extensive security and supply chain risks with its desire for closer economic ties with China. It should, for example, be more proactive in raising the issue of Beijing's ongoing support for Moscow continuing to pursue its war in Ukraine. Additionally, when signing new international treaties and economic agreements, the Government should commit to publishing an accompanying statement which makes it clear how national security considerations have been accounted for in detail. These assessments should make sure to include examination and mitigation of emerging challenges including, but not limited to, espionage, transnational repression and AI-enabled harms. (Paragraph 105).

We are taking a long-term, strategic approach, rooted in the UK national interest. We recognise that China poses a series of threats to UK national security, and we challenge these robustly – from cyber-attacks, foreign interference and espionage targeting our democratic institutions, to transnational repression of Hong Kongers and China's support for Russia's invasion of Ukraine.

We are also alive to the fact that China presents the UK with opportunities as the world's second largest economy and the UK's third largest trading partner. We will therefore continue to develop a consistent and pragmatic approach to economic engagement, without compromising our national security.

The Government will not hesitate to use our powers to protect national security wherever we identify concerns. We have a range of effective measures in place, including the National Security and Investment Act, which gives the Government powers to intervene in acquisitions that may give rise to risks to the UK's national security. We will increase our focus towards promoting industries and technologies that drive economic growth, while securing supply chains in critical and important sectors. Our new Industrial Strategy and Trade Strategies are central to this.

We engage China regularly on its political and military backing for Russia, including the provision by Chinese companies of dual-use goods and support to Russia's military industrial complex, including at Prime Minister and Foreign Secretary-level and, most recently, during the Prime Minister's visit to Beijing in January 2026.

When meeting Xi Jinping and Premier Li Qiang in January 2026, the Prime Minister called on China to end economic support for Russia's war effort, including companies providing dual-use technologies, and urged them to use their influence on Putin to end his aggression in Ukraine.

The transatlantic alliance and UK security

Conclusion: The UK has strategic dependencies on the United States for core capabilities in nuclear, intelligence and conventional defence. While it is positive that the Government has recognised the need for the UK to prepare for a future where the United States makes a less active contribution to European security, more must be done to ensure Europe and the UK are better able to protect themselves. At the same time, the UK should continue communicating to the United States about the mutual benefits of the US-UK security relationship and ensure that areas of national strategic importance are not undermined by other challenges (for example, US-led peace negotiations over Ukraine, or commitments to the situation in Iran). (Paragraph 118).

Recommendation: As well as continuing its strategic collaboration with the United States where practical, the Government must also develop a clear plan, along with other European allies, for a transition towards greater European leadership of NATO. Preparing for a 'worst-case scenario' whereby Europe can no longer rely on US support in the event of a crisis, the Government must work with European partners to invest in its own capabilities to offset this potential withdrawal. (Paragraph 119).

Recommendation: The Government should also pursue this contingency through continuing to develop strategic partnerships with non-NATO allies in other parts of the world. In addition to working to shore up

European NATO's capabilities, the UK should plan to move away from a bilateral relationship with the United States that is so dependent on the latter for nuclear and intelligence operations, and conventional defence. (Paragraph 120).

The depth and breadth of the UK-US defence and security relationship delivers mutual benefits for both nations. As the Prime Minister said in his speech at the Munich Security Conference, the emphasis should be on interdependence and not overdependence. NATO members need to answer the call for more burden-sharing in Europe.

The UK is playing a leading role, cooperating with NATO, the US, and European counterparts to strengthen Euro-Atlantic Security. This collaboration is being further reinforced through a series of bilateral treaties intended to reinforce our collective security and defence industrial partnerships, including the 2025 Lancaster House 2.0 Treaty with France, and the Kensington House Treaty with Germany.

The US remains the UK's most important defence and security ally. We are committed to a strong and enduring NATO alliance, which benefits the security and prosperity of all its members, including the United States. We are working closely with our allies to build a stronger, more capable European pillar within NATO, ensuring the alliance remains the bedrock of transatlantic security. This generational shift in defence investment and industrial cooperation is designed to strengthen NATO, and move away from overdependence on any one state. We are already enhancing nuclear cooperation with France, working with our Joint Expeditionary Force allies to protect our northern flank, and developing next generation long-range missiles in partnership with Germany, France and Italy.

'NATO First' does not mean 'NATO only' and we are deepening our alliances and partnerships across the world. Major capability programmes and industrial agreements like AUKUS, the Global Combat Air Programme, and the Defence Industrial Roadmap with India and our Strategic Partnership with Indonesia complement but are not tied to NATO. This means we are able to diversify our relationships and reduce our dependencies on any single state. To ensure that our alliances remain robust we are also increasing the sovereign strengths of the UK that underpin our national security, including the launch of a £500 million Sovereign AI Fund and a £1 billion programme to procure commercial-scale quantum computers.

International Partnerships

Conclusion: We welcome the Government's efforts to diversify partnerships, illustrated by deepening trade and security collaboration with India and engagements with Gulf countries. This work is crucial both to ensuring the UK can draw on breadth and depth in its partnerships to support economic growth, and improve resilience during periods of heightened international tension. Recent support by the UK in deploying the RAF to the collective self-defence of Gulf countries in the face of Iranian strikes is welcome. (Paragraph 125).

Recommendation: The Government should continue to ensure that sensible trade-offs are made between economic growth and national security objectives as it pursues new strategic relationships and bolsters existing ones. The scale of this work should be expanded, and its speed accelerated. (Paragraph 126).

The Government agrees that we should continue to pursue new strategic relationships and bolster existing ones. The National Security Strategy aims to sharpen our diplomatic focus on geographically dispersed, economically vibrant, fast-growing, and advanced economies. To those ends, the government has delivered a range of new and significant partnerships including the UK-Japan Industrial Strategy Partnership, the Strategic Partnership with Indonesia and the UK-India Trade deal. These nations share an interest in counteracting economic coercion and preventing the fragmentation of the international economic order.

Furthermore, we are committed to fostering trade and investment relationships that actively promote secure, resilient growth and provide a boost to the UK economy. Key instruments for mitigating national security risks in this context are the National Security and Investment Act and supporting the establishment of an Economic Security Advisory Service.

Changing nuclear context

Conclusion: A credible, sustainable and independent UK nuclear deterrent is integral to UK national security, and as a buffer against allied proliferation in an era of fast-changing nuclear risks. (Paragraph 135).

Recommendation: The Government would benefit from having a more open public conversation about nuclear threats, spending choices and future nuclear security programmes. It should set out how it plans to extend UK-France collaboration on nuclear security. (Paragraph 136).

The Government agrees with the Committee's conclusion. The National Security Strategy and SDR outlined the threat picture and the UK's intention publicly. A further £6bn was announced through the SDR to upgrade our

nuclear submarine production facilities. This will support tens of thousands of jobs in Barrow, Derby and Sheffield and will ensure we have the capacity to build a larger fleet of more capable submarines at a quicker rate than before; a new submarine every 18 months. The UK has also deepened nuclear cooperation with France, as set out in the Northwood Declaration, including stating that while our nuclear forces are independent, they can be coordinated.

Which capabilities to prioritise?

Conclusion: The National Security Strategy is clear that sovereignty over certain national security capabilities, including nuclear, emerging technologies, shipbuilding and steelmaking, is important. However, beyond this, there is no clear definition of how the Government defines what it considers to be a sovereign capability. Nor is there sufficient indication of what specific capabilities and technologies the Government intends to prioritise as part of this work. (Paragraph 151).

Conclusion: We appreciate that the definition of sovereignty will differ by sector and by degree. However, the general lack of clarity on definitions and objectives complicates research and development planning and investment. The UK has a strong base of talent and skills in emerging technologies—artificial intelligence in particular—where some level of sovereignty will be desirable and the Government must ensure that this advantage is utilized. (Paragraph 152).

Recommendation: The Government should provide a clear, written definition of what a sovereign capability is, including different levels of sovereignty. The Government should also outline which specific existing and emerging technologies it is seeking to develop, and to what level of sovereignty. These definitions should be informed by risk assessments of critical supply chains, critical minerals and investment, and export security, and should be agreed across government. Relevant departments must have regard to these definitions when making any decisions around investment and support both for firms developing sovereign capabilities and for higher education institutions researching emerging technologies. (Paragraph 153).

Recommendation: Additionally, the Government should set out the order of priorities for the different sovereign capabilities it intends to develop. The Defence Investment Plan would be a useful place for this, as a signal to industry. (Paragraph 154).

In a rapidly evolving global landscape, where dependencies are increasingly weaponised, our approach to sovereign capability must be dynamic. Instead of a strict definition we need a flexible approach which takes account of multiple factors, including but not limited to those listed by the committee, and which adapts to changes over time.

Any published list risks becoming outdated as technologies advance, and risks inadvertently telegraphing our specific vulnerabilities to hostile actors or signalling areas of strategic strength to competitors.

Businesses need clarity and certainty to invest. We are delivering that certainty not through a restrictive list, but through our strategic frameworks. Our Industrial Strategy provides clear, long-term signalling to industry on our priority eight high-growth sectors, as well as the foundational sectors on which they rely. Alongside this, the National Security and Investment Act (NSIA) provides a robust, predictable, and transparent regime for businesses, clearly outlining the 17 sensitive areas of the economy where we will safeguard assets from hostile foreign investment. The DIP will also set out the UK's capability priorities for the next ten years, providing a clear signal to industry.

Defence industrial base

Conclusion: Industry lacks an adequate signal from Government on the allocation of spending across the defence, security and resilience sectors. This impacts the ability to plan research and development spending in a way that aligns with Government objectives, and prioritises the most important sovereign technologies. For SMEs in particular, this contributes to their vulnerability to acquisition by foreign investors, compromising their ability to contribute to security and sovereignty goals. (Paragraph 163).

Recommendation: The Defence Investment Plan must be completed and published as soon as possible. Within the Plan, the Government should provide further detail on the funding mechanisms it will use to support firms as it seeks to revitalise the UK's defence-industrial base and develop sovereign capabilities. SMEs in particular need further financial support and guidance to grow and develop capabilities and avoid the risk of homegrown talent and capabilities being acquired by foreign investors. (Paragraph 164).

The MOD's forthcoming Defence Finance and Investment Strategy will set out measures to improve SMEs' access to finance and growth capital. The Department is also committed to publishing an ambitious SME action plan, alongside a direct spending target, once the Defence Investment Plan is finalised.