House of Lords
House of Commons

Joint Committee on the National Security Strategy

The National Security Strategy

Fourth Report of Session 2024–26 HC 1045/HL Paper 281

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, together with formal minutes relating to the report, was Ordered by the House of Commons and House of Lords, on 23 March 2026, to be printed. It was published on 27 March 2026 by authority of the House of Commons and House of Lords.

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 telephone number for general enquiries is 0207 219 4043; the Committee's email address is jcnss@parliament.uk. You can follow the Committee on X (formerly Twitter) using @JointCtteNSS.

Contents

Executive Summary

The assumptions underpinning the UK's national security are being challenged to an unprecedented degree. The National Security Strategy (NSS) recognises that the UK is now living through an era of radical uncertainty, with the assumptions underpinning UK security undergoing a fundamental change. Great power competition, a more transactional approach to managing relationships and conflict, and the proliferation of hybrid attacks facilitated by emerging technologies, are chipping away at the normal barriers to aggressive and risky behaviours by both hostile and friendly states.

Our inquiry set out to scrutinise the 2025 National Security Strategy with respect to its overall approach and coherence across Government, aiming to understand conditions for success and key obstacles to delivery.[1] Most pressingly, we found that there is a gap between the commitments made in the NSS and how the Government intends to deliver these. We are unclear on the adequacy of cross-Government accountability, and funding for commitments. A detailed plan for the development of sovereign capabilities is also lacking.

We found that gaps in the consultation and engagement process which informed the development of the NSS may have led to a lack of focus on the impact of cuts to the UK's soft power capabilities, and the potential consequences of this for security abroad and at home. Throughout the inquiry, we encountered a distinct lack of clarity over which Government departments are responsible for which aspects of national security, and that Cabinet Office mechanisms for oversight may not be sufficiently robust to ensure coherent implementation of national security policy across Government.

While the NSS identifies the need to boost civil resilience against the proliferation of hybrid threats, we found that detail for plans around bolstering the protection of critical national infrastructure (CNI), the remit of the recently-formed UK Resilience Academy, and the vision for a national conversation to develop a whole-of-society approach to security and resilience is lacking. Critical stakeholders, including operators of CNI and public sector bodies, require greater guidance and support to ensure they are able to adapt to a more dangerous threat environment.

1 There are likely to be impacts for UK national security of US-Israeli strikes on Iran since 28 February 2026, Iranian retaliation and the effective closure of the Strait of Hormuz. These events took place after we had finished taking evidence for this report.

Evidence we received largely aligned with the Government's view that increasing global tensions present a threat to UK security, and that more must be done to reduce dependence on the United States—for security capabilities and intelligence sharing—and China—for the supply of critical minerals and other products—and build capability through collaboration with partners in Europe and elsewhere. But the Government should be doing more as part of these efforts, reflecting the way in which existing partnerships and alliances are fundamentally changing.

Furthermore, the Government does not have a clear definition of sovereign capabilities, which the NSS identifies as necessary to develop in order to mitigate dependencies on partners for defence and security assets and systems. This lack of clarity complicates research and development planning and investment, and there is a need for a clearer steer to industry to ensure defence and security companies' efforts align with the Government's objectives in this respect.

We are calling for:

- Greater Government transparency on national security issues, through annual updates to our Committee; more robust engagement with stakeholders; and more detail on the planned 'national conversation' on security and resilience;
- Robust internal accountability mechanisms to ensure that Government departments stick to their commitments regarding national security policy;
- Greater clarity over the target to spend 1.5% of GDP on security and resilience by 2035;
- More detail on plans for bolstering the protection of critical national infrastructure (CNI), including plans for reform of the Armed Forces Reserves and new burdens for CNI operators arising from the Cyber Security and Resilience Bill;
- Developing a clear plan for greater European leadership of NATO and preparing for a worst-case scenario where Europe can no longer rely on US support in the event of a crisis;
- Ensuring momentum in imposing ever greater costs on Russia is maintained, as long as it continues its war in Ukraine and acts of hybrid aggression against the UK and allies;
- Recognising that China presents a clear national security threat, and committing to greater transparency around how security is prioritised in the UK's relationship. For example, when signing new international

treaties and economic agreements with China, the Government should publish an accompanying statement on how national security considerations have been accounted for;

- Building on the Northwood Declaration by extending UK-France collaboration on nuclear;
- Strengthening the signal from Government to industry on the allocation of spending across the defence, security and resilience sectors, providing detail on funding mechanisms and dedicated support to security-focussed Small and Medium-sized Enterprises; and
- Defining 'sovereign capabilities' and the differing levels of sovereignty required for specific technologies.

1 Our inquiry

Our inquiry

1. We launched this inquiry in June 2025 to examine the National Security Strategy (NSS), published in the same month. The NSS is the Government's strategic policy document designed to "identify the main challenges we face as a nation", "describe the key principles underlying the government's approach to these challenges" and "explain the actions the government will be taking in response."[2] It outlines the Government's plans to deal with the proliferation of serious threats to the UK's security, ranging from hybrid attacks and cybercrime to economic insecurity.[3]

2. Our objective was to assess the NSS's overall approach and coherence across Government, aiming to understand conditions for success and key obstacles to delivery, and to identify spending priorities.

Our report

3. This report focuses on the most urgent security challenges that the Government must address. Given the breadth of national security as a policy area, it aims to build on, rather than duplicate, relevant work by other committees.[4] There are likely to be impacts for UK national security of US-Israeli strikes on Iran since 28 February 2026, Iranian retaliation and the effective closure of the Strait of Hormuz. (These events took place after we had considered the relevant evidence: the Committee may return to this topic in due course.)

4. In recent years, there have been many challenges to the assumptions underpinning UK and European security: Russia's full-scale invasion of Ukraine in 2022; rapid developments in the sophistication of AI and other frontier technologies; and the re-focussing of US priorities away from

2 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, gov.uk (accessed 6 March 2026)

3 NB: The inquiry did not examine the ramifications of the United States' National Security Strategy specifically as this was published following the gathering of most of the inquiry's evidence in November 2025. There is, however, consideration throughout of how the UK negotiates its changing security relationship with the US.

4 For example, the Defence Committee's report on the UK contribution to European security and the Home Affairs Committee's inquiries discussed in paras 73 and 49 respectively.

Europe and towards the Americas and the Indo-Pacific, as outlined in its National Security Strategy.[5] These have contributed to what the Government describes in the NSS as "an era of radical uncertainty".[6] We are hopeful that our findings, conclusions and recommendations will help the Government better navigate this continuing uncertainty.

5. This report is structured in the following way:

a. Chapter 2 considers the development process of the NSS itself, identifying issues with sequencing, transparency and consultation. It recommends that the Government improve its level of transparency and engagement with stakeholders, civil society and the public, as well as addressing potential assessment gaps regarding the impacts of diminishing UK soft power.

b. Chapter 3 considers the oversight and implementation of the strategy, identifying potential gaps in cross-government working and funding for delivery. It recommends the Government clarify oversight mechanisms for delivery and funding of the NSS.

c. Chapters 4–6 assess elements of each "pillar" of the NSS: respectively, Security at Home; Strength Abroad; and Sovereign Capabilities. We make recommendations that include providing greater detail on the Government's plans for protecting critical national infrastructure and assessing civil preparedness; providing greater transparency on how it is managing the national security risks it faces in its relationships with China and the US; and giving clearer direction to industry in how it defines sovereign capabilities, and what support will be available for firms to help develop these.

d. Annex 1 summarises the results of a private event on Russia hosted by the Committee in January 2026, which convened experts and former diplomats. This event was held to consider the security threat posed by Russia and to explore and challenge assumptions relating to Russia, including with reference to the National Security Strategy, Strategic Defence Review and other strategy documents. The event results informed this inquiry's recommendations.

5 The White House, National Security Strategy of the United States of America, November 2025
6 HM Government, National Security Strategy, gov.uk, June 2025, p 4

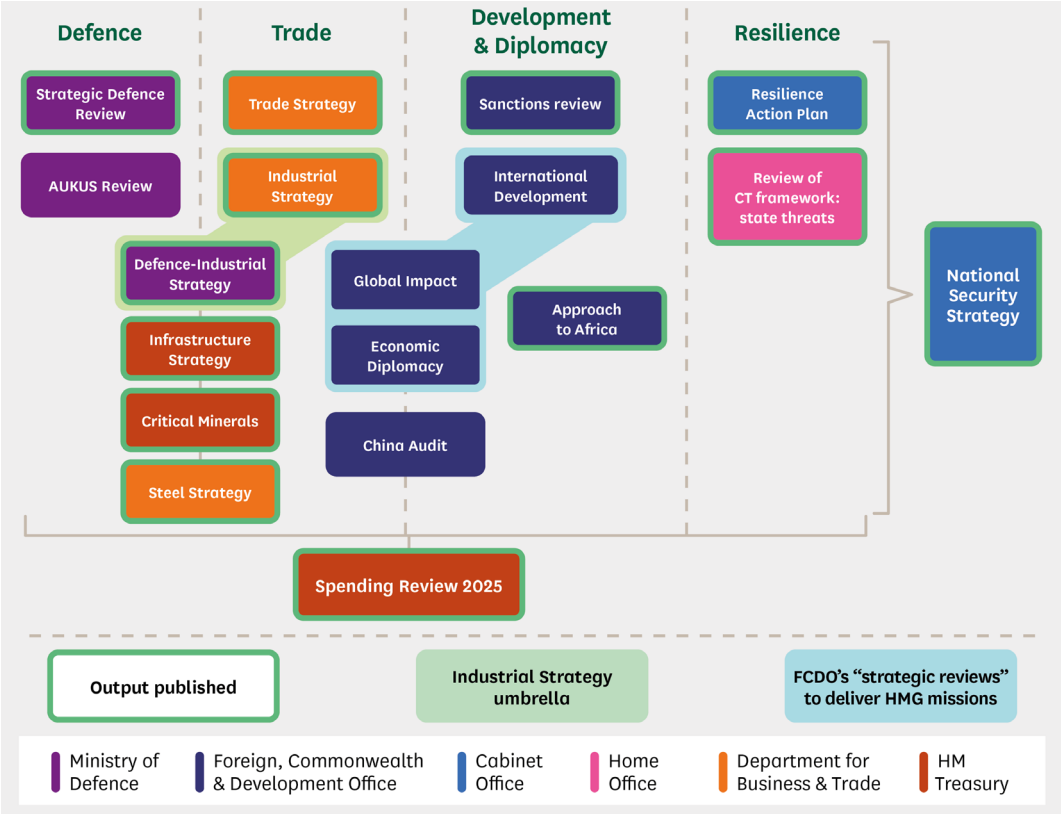
NSS assessment of the strategic context

6. According to the NSS, the security threats facing the UK are proliferating and intensifying.[7] These range from hybrid to conventional warfare; terrorism; biosecurity; and the rapid and uncontrolled pace of emerging technologies. Russia presents the single greatest source of threats to the UK's security, with China and Iran also presenting strategic challenges.

7. A number of strategy and policy documents informed the NSS. Some, including the upcoming Research Security Strategy[8] and the Energy Resilience and Security Strategies,[9] will likely inform adjustments to national security policy on an ongoing basis. Funding allocated for the delivery of the NSS was set at the 2025 Spending Review which laid out the Government's plans for reaching a spend of 2.6% of GDP on defence by 2027[10] as well as spending in relation to its commitment to spend 1.5% of GDP on security and resilience by 2035 (discussed in more detail in Chapter 3).

7 HM Government, National Security Strategy, gov.uk, June 2025, p 8
8 Research: Cybersecurity UIN 93076, 28 November 2025
9 National Energy System Operator (TNS0031)
10 HM Treasury, Spending Review 2025, gov.uk, 30 June 2025, pp 2; 17

Figure 1: Strategy and policy documents informing the National Security Strategy (non-exhaustive)



Note: Analysis and infographic produced to visualise different documents relating to the 2025 National Security Strategy. This analysis is not designed to be exhaustive. "Output published" has been judged according to whether a discrete output has been published from a specific review/policy process.

NSS objectives

8. The NSS seeks to draw together the UK's national security objectives and the means to achieve these. It has a focus on the growing concern for collective European security in the face of the US's changing strategic priorities and continued Russian aggression.[11] It also points to increasing great power competition between the US and China, causing cascading challenges across trade, technology development and defence partnerships and locates the Indo-Pacific and the Middle East as other areas of high tension.[12]

11 HM Government, National Security Strategy, gov.uk, June 2025, p 18, p 31
12 HM Government, National Security Strategy, gov.uk, June 2025, pp 35–36

9. The Government outlines ambitions to:

- **a.** improve 'security at home' by upgrading domestic resilience and defensive capabilities;[13]
- **b.** have greater 'strength abroad'; prioritising European collective security through leadership in NATO and building new capability partnerships with third-party countries;[14] and
- **c.** develop 'sovereign and asymmetric capabilities', through rebuilding the UK's defence industrial base, reducing reliance on others.[15]

10. Detail on how these aims will be delivered is provided in accompanying strategy and review documents, including the Strategic Defence Review;[16] Resilience Action Plan;[17] the Defence Industrial Strategy;[18] the 10-Year Infrastructure Strategy;[19] and the Government Cyber Action Plan.[20]

11. Our report outlines some conceptual difficulties with the NSS. For example, the NSS has a significant focus on harnessing hard power, and clearly acknowledges the risks of overseas instability—but says less about the options for prevention. There is limited focus on the use of soft power as an asymmetric advantage to be deployed too. The level of detail on regional interests is also varied, meaning the NSS does not always lend itself to detailed analysis to areas of relevance to national security (such as the Arctic, Africa and the Middle East). We examine the implications of these issues throughout this report.

13 HM Government, National Security Strategy, gov.uk, June 2025, pp 21–28
14 HM Government, National Security Strategy, gov.uk, June 2025, pp 29–40
15 HM Government, National Security Strategy, gov.uk, June 2025, pp 41–50
16 Ministry of Defence, Strategic Defence Review
17 HM Government, The UK Government Resilience Action Plan, 8 July 2025
18 Ministry of Defence, Defence Industrial Strategy 2025: Making Defence an Engine for Growth, 8 September 2025
19 HM Treasury and National Infrastructure and Service Transformation Authority, UK Infrastructure: A 10 Year Strategy, gov.uk, 19 June 2025
20 Department for Science, Innovation and Technology, Government Cyber Action Plan, gov.uk, 20 March 2026

2 National Security Strategy development process

12. In this chapter, we identify issues with how the National Security Strategy (NSS) was developed, which may undermine its overall prospects of success. We consider these given their importance to stakeholders, whose buy-in will be essential to realising the ambition for a "whole-of-society"[21] approach to defence, security and resilience.[22]

13. Getting the strategic outlook and plan for delivery right at this stage will be crucial in securing the UK's security in the long-term. This will be easier to facilitate if Government departments, intelligence and security agencies, the armed forces, relevant stakeholders in the private sector and the public are pulling in the same direction by seeing evidence of—and buying into—a more robust approach to national security and resilience.

14. Firstly, we consider the work to engage with stakeholders as the strategy was developed, finding gaps in consultation and transparency processes. We then look at how the sequencing of the NSS after the Strategic Defence Review (SDR) may have led to a lack of focus on the impact of cuts to the UK's soft power capabilities, including development assistance.

Engagement with stakeholders

Consultation

15. Some stakeholders argued that consultation for the NSS was less extensive than that for the SDR. Rethinking Security told us the external engagement undertaken by the Government "consisted only of a few roundtables of experts" from think tanks and universities and that civil society organisations were "otherwise absent", representing a missed opportunity to bring stakeholders along with the formulation and delivery of national security objectives.[23] Trade body techUK told us there had been a "shortage of formal engagement with the private sector and notably the tech industry"

21 Ministry of Defence, Strategic Defence Review, pp 86–93

22 Q41, Q46

23 Rethinking Security (TNS0015)

and that the Government should "conduct widespread engagement with industry" to help rectify this,[24] a point echoed by defence companies Roke and Cunning Running Software Ltd.[25]

Transparency

Timelines

16. Some stakeholders, including techUK and Cunning Running Software Ltd, suggested that the NSS could have been more transparent on delivery timelines.[26] The National Preparedness Commission told us that documents accompanying the NSS, such as the Resilience Action Plan, should provide this additional detail on specific areas of the strategy.[27] The SDR, by contrast, has a more detailed set of timelines accompanying its recommendations.

17. We understand that the lack of timings for NSS delivery does not necessarily mean the Government has not established its own milestones internally, and that there may be legitimate security reasons why it chose not to publish these. However, it represents a challenge in scrutinising progress and holding the Government to account.

China Audit

18. The Government's China Audit was designed to "deliver a long-term strategy" regarding China, given the "inescapable fact" of Chinese power and previous approaches being "completely inadequate."[28] The Audit was completed in June 2025 but was not published; then-Foreign Secretary, Rt Hon David Lammy MP, told the House of Commons "most of the detail is not disclosable without damaging our national interests."[29]

19. There was strong support from witnesses to our inquiry for the Government to publish a version of the China Audit, including former Governor of Hong Kong, Lord Patten of Barnes. Lord Patten told us that not publishing the

24 techUK (TNS0020)
25 Cunning Running Software Ltd (TNS0028); Chemring Group Plc/Roke Manor Research Limited (TNS0026)
26 ADS Group (TNS0007); techUK (TNS0020)
27 National Preparedness Commission (TNS0001)
28 Foreign, Commonwealth and Development Office, China audit: Foreign Secretary's statement, gov.uk, 24 June 2025
29 Foreign, Commonwealth and Development Office, China audit: Foreign Secretary's statement, gov.uk, 24 June 2025

Audit would not help "government [or] local government, universities and [technology] firms to co-ordinate how we deal with China".[30] Lord Patten told us:

> It would be crazy for us to think that we should publish an audit and not let most of the people who would benefit from reading it actually see it.[31]

20. Defence and security trade association ADS Group also warned that the lack of a published China Audit was not helping industry understand the Government's approach to China.[32]

21. **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.

22. **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.

23. **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.

30 Q77
31 Q78
32 ADS Group (TNS0007)

Soft power, development and national security

24. There was consensus in evidence that the NSS provides a good analysis of the threats facing the UK. ADS Group, for example welcomed its "broad scope and emphasis on resilience, technology, and domestic capability".[33] The Centre for Long Term Resilience also welcomed the "focus on resilience as a national priority".[34] techUK said it "set a bold and necessary tone", representing "a welcome breakdown of the serious threats facing the UK and presents a stark warning that the country must prepare for the possibility of direct attack."[35]

25. Some stakeholders suggested it is not clear how the Government intends to tackle the root causes of insecurity that it identifies in the NSS, in particular the proliferation and escalation of conflict. These stakeholders[36] argued that this was partly due to the decision to publish the NSS after the SDR, resulting in a focus on UK 'hard' capabilities at the expense of non-defence aspects of national security such as conflict prevention.[37]

26. The Government plans to reduce funding for Official Development Assistance (ODA) from 0.5% to 0.3% of Gross National Income from 2027, to be put towards improving the UK's hard power.[38] This follows on from reductions to the ODA budget by previous Governments.[39] In oral evidence to the International Development Committee, Baroness Chapman, Minister of State for International Development and Africa, said that this decision was taken because there "was a need to find money quickly to commit to defence".[40]

27. ODA cuts have impacted many regions of the world, with cuts being made simultaneously by other Western nations: the US in particular.[41] Witnesses to our inquiry raised two key risks from this reduction: firstly, that of a negative impact on conflict prevention efforts in unstable regions and secondly, the growth of the Russian and Chinese influence in these regions, as discussed in the following sections.

---

33 ADS Group (TNS0007)
34 The Centre for Long Term Resilience (TNS0009)
35 techUK (TNS0020)
36 Rethinking Security (TNS0015); Saferworld (TNS0017)
37 Gender Action for Peace and Security (TNS0021)
38 House of Commons Library, Research Briefing 10243, UK aid: Reducing spending to 0.3% of GNI by 2027/28, 24 February 2026
39 The previous Government reduced aid spending from 0.7% of GNI to 0.5% of GNI in 2020—House of Commons Library, Research Briefing 9224, UK aid: spending reductions since 2020 and outlook from 2024/25, 12 February 2025
40 Oral evidence taken by the International Development Committee on 20 January 2026, Q146
41 Chatham House, First USAID closes, then UK cuts aid: what a Western retreat from foreign aid could mean (accessed 4 March 2026)

Official Development Assistance (ODA) cuts and conflict prevention

28. Civil society organisations highlighted the lack of focus in the NSS on the implications of ODA cuts, including on conflict prevention and the risks of spillover to UK security.[42] The HALO Trust argued that reductions in the development budget have "constrained the UK's ability to deliver a balanced and sustainable security strategy" and that there is a risk that security ends up "overlooking the value of non-military interventions that are often most effective at preventing conflict and building resilience".[43]

Growing Russian and Chinese influence

29. Witnesses to our inquiry warned of the potential growth in Russian and Chinese influence in areas where ODA has been reduced, in particular within Africa. Dr Marion Messmer, Director of the International Security Programme at Chatham House, told us that the UK and allies should "not underestimate the Russian presence in Africa and Russian strategic interests there" and that aid drawdown from the UK and allies is "leaving a lot of diplomatic space open to Russia and China".[44] Rose Goettemoeller, former Deputy Secretary General at NATO and Under Secretary of State for Arms Control and International Security at the US State Department, suggested that European partners should be looking to "step into the breach where some [US-funded] programmes have been closed" by President Trump's administration, in order to help counter "Chinese and Russian influence in the global South".[45]

30. The ability to counter the growth in this influence through British soft power has the potential to be further undermined by uncertainty over the future funding of organisations such as the British Council.[46] The Foreign Secretary announced on 20 March 2026 that funding of the BBC World Service would be increased by £11m a year, for the next three years.[47]

42 Rethinking Security (TNS0015); Saferworld (TNS0017); Gender Action for Peace and Security (TNS0021)
43 The HALO Trust (TNS0019)
44 Q63
45 Q64
46 Oral evidence taken by the Foreign Affairs Committee on 19 November 2024 and 28 October 2025
47 Foreign, Commonwealth and Development Office, Foreign Secretary on International Development: 19 March, 19 March 2026

31. In January 2025, the Government created the Soft Power Council, an advisory board to the UK Government that brings together experts to shape the UK Government's soft power strategy and impact.[48] Over one year since, it is not clear how frequently the Council has met, what the outcomes of its advice have been, or how the Government is making the most of this expertise. Given that the National Security Strategy does not focus much on soft power, greater clarity over the Council's work now would enable external organisations important to UK soft power to understand the Government's strategic priorities. Greater clarity would also support parliamentary scrutiny, in particular by the Foreign Affairs Committee.

32. **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.

33. **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.

48 Foreign, Commonwealth and Development Office and Department for Culture, Media and Sport, UK Soft Power Council: membership and terms of reference, gov.uk (accessed 6 March 2026)

3 Oversight and implementation

34. In this chapter, we consider the Government's arrangements for oversight and implementation of the National Security Strategy (NSS). This includes internal mechanisms for overseeing and ensuring delivery between the Cabinet Office, different Government departments and the broader national security apparatus. We then consider how the Government intends to fund its national security commitments through examination of the aim to spend 1.5% of GDP on security and resilience by 2035.

Delivery: Ownership and responsibilities

35. While the Cabinet Office and the Chancellor of the Duchy of Lancaster (CDL) have oversight for cross-Government delivery of national security policy, individual departments have responsibility for specific areas under their remit, with Ministers attending National Security Council (NSC) meetings, chaired by the Prime Minister.[49] Within national security planning, a 'Lead Government Department' model is employed, whereby these departments are responsible for "leading work to identify serious risks and ensuring that the right planning, response and recovery arrangements are in place."[50] However, beyond the role of the Security Minister in the Home Office,[51] it is unclear which responsibilities within the NSS have been assigned to which departments.

36. In July 2025, then-CDL the Rt Hon Pat McFadden MP told us that the NSC is the "principal cross-government forum" for national security "which will drive all this through", bringing together different departments with security

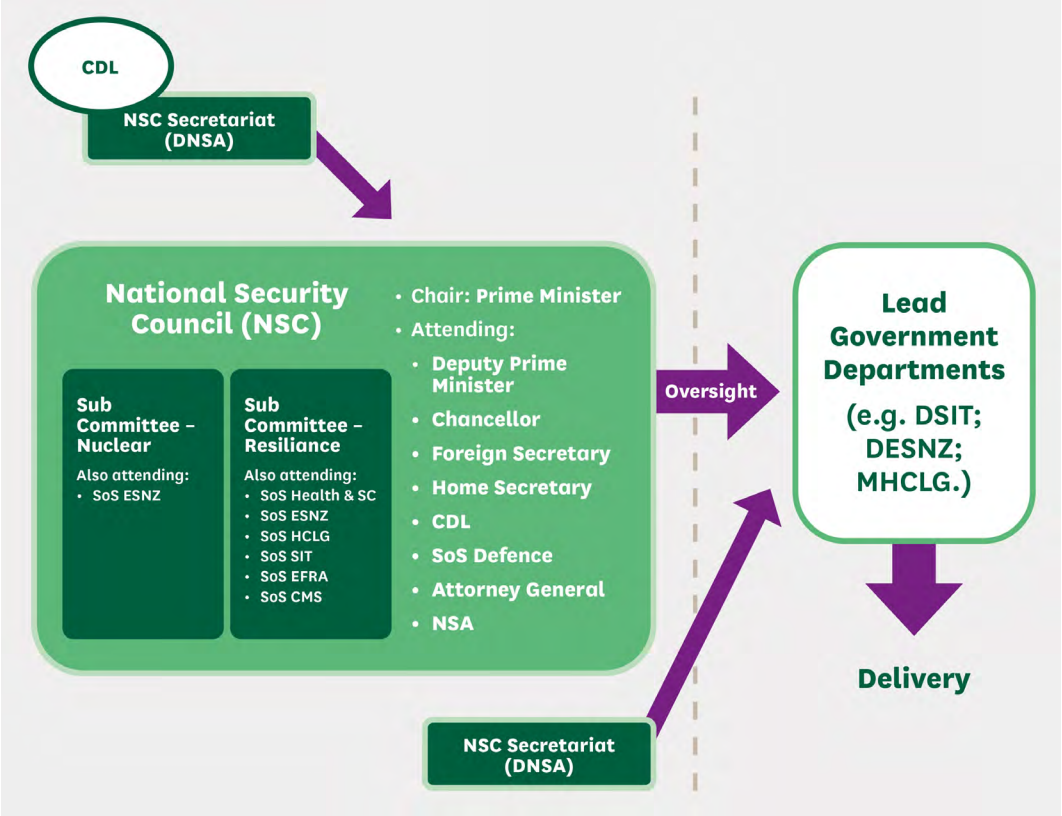
49 These include Ministers from: The Foreign, Commonwealth and Development Office; The Ministry of Defence; The Department for Business and Trade; The Department for Science, Innovation and Technology; The Department for Health and Social Care; The Department for Energy Security and Net Zero; The Ministry of Housing, Communities and Local Government; The Department for Environment, Food and Rural Affairs and the Department for Culture, Media and Sport.

50 Cabinet Office, The Roles of Lead Government Departments, Devolved Administrations and Other Public Bodies, gov.uk (accessed 6 March 2026)

51 Responsibility for: Counter-terrorism & extremism; State threats; Cyber security & crime; Serious organised crime; Maritime & aviation security – Home Office, Minister of State (Minister for Security), gov.uk (accessed 24 February 2026)

responsibilities.[52] The National Security Adviser and the Deputy National Security Advisers lead the Secretariat of the NSC, acting as the main co-ordinators "on security, intelligence, defence and some foreign policy matters".[53]

Figure 2: Cross-Government national security apparatus



NB: Infographic produced through analysis of evidence to this inquiry and information provided on the Cabinet Office website: Cabinet Office, List of Cabinet Committees, gov.uk (accessed 4 March 2026). The Cabinet Office has multiple Committees across a range of policy areas. The above only covers the National Security Committee and its two sub Committees (Resilience and Nuclear).

37. The Lead Government Department model has faced criticism, including from our predecessor Committee, which highlighted the limited oversight and lack of accountability on whether departments are prioritising security and resilience goals.[54] Additionally, we have not been able to publicly question the National Security Adviser about delivery of national security policy, in contrast to all previous parliaments under all previous administrations: an indisputable barrier to effective scrutiny. This situation was further exacerbated when the Department for Science, Innovation and Technology

52 Q27
53 Institute for Government, National security adviser (accessed 16 February 2026)
54 Letter from the predecessor Committee to the Deputy Prime Minister and Chancellor of the Duchy of Lancaster regarding resilience, 14 June 2023

declined to provide a minister to appear alongside the Chancellor of the Duchy of Lancaster and Security Minister at the concluding evidence session for this inquiry.[55]

38. This model of oversight may also contribute to what some industry witnesses characterised as "fragmented initiatives" when it comes to the Government approach to civil resilience, and a lack of clarity in how the NSS will embed a cross-Government approach with industry when implementing the plan.[56] techUK, for instance, highlighted the need to define cross-cutting departmental responsibilities better, assigning "department leads to certain delivery ambitions".[57] These points echo concerns raised in our 'Subsea telecommunications cables: resilience and crisis preparedness' report regarding the efficacy of cross-Government working, where we concluded that "improvements to oversight and co-ordination would benefit day-to-day work and crisis response."[58]

39. The House of Commons Defence Committee has previously called for the creation of a separate Minister of Homeland Security to provide better clarity of oversight and accountability for delivery, although the CDL told us that he did not see the case for this, saying that the Cabinet Office already fulfils a cross-Government coordination function.[59]

40. **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.

55 The Department for Science, Innovation and Technology (DSIT) declined to provide a minister for this session in January 2026 on the grounds that each department should lead on the science and technology-related national security areas within its remit, making this a cross-HMG endeavour rather than a DSIT-exclusive one. The Secretary of State subsequently agreed to appear before the Committee, but it was not possible to find a suitable date for the Secretary of State to appear before the publication of this report.

56 Thales UK Limited (TNS0027)

57 techUK (TNS0020)

58 Joint Committee on the National Security Strategy, First Report of Session 2024–26, Subsea telecommunications cables: resilience and crisis preparedness, HC 723, para 162

59 Q132

41. **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.

42. **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.

Funding

43. The Government is planning to spend 1.5% of GDP on resilience and security as part of the wider commitment made by NATO allies in June 2025 to spend 5% of GDP on defence and security by 2035.[60] It is not clear what additional resilience capabilities—for instance, improvements to the physical and cyber security of critical national infrastructure—will be included in the target, which the Government says it will hit by 2027.[61] The CDL indicated to us that, as of 2027, the spend will represent "things that we are currently doing", reflecting allocations from the 2025 Spending Review, and that "additional capability will come in future years".[62] The Institute for Fiscal Studies have reported that Government statements have suggested that meeting the 1.5% target "will not require an increase in total spending, although it may affect how individual departments' budgets are allocated."[63]

60 NATO, Defence expenditures and NATO's 5% commitment (accessed 4 March 2026); NATO, The Hague Summit Declaration (accessed 4 March 2026)
61 Q116
62 Qq 118–119
63 Institute for Fiscal Studies, UK defence spending: composition, commitments and challenges, 26 September 2025

44. Industry bodies and defence companies told us of the need for greater clarity on what spending counts towards the 1.5% target,[64] to incentivise industry to invest in relevant research and development.[65] Defence company Northrop Grumman UK told us that spending must include that which "genuinely strengthens UK security and resilience",[66] and Thales UK Limited, another defence company, told us it should include securing defence supply chains and protecting critical infrastructure.[67]

45. In addition to the 1.5% security and resilience spending target, the Government has additional spending plans, which will in theory feed into bolstering security and resilience capabilities. The 10-Year Infrastructure Plan, for instance, aims to strengthen resilience standards across critical national infrastructure, including "additional standards where necessary" by 2035–36.[68] However, it is not wholly clear where funding will come from for these upgrades, once the new standards have been put in place.

46. **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.

47. **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.

64 ADS Group (TNS0007); Northrop Grumman UK (TNS0018)
65 ADS Group (TNS0007)
66 Northrop Grumman UK (TNS0018)
67 Thales UK Limited (TNS0027)
68 HM Treasury and National Infrastructure and Service Transformation Authority, UK Infrastructure: A 10 Year Strategy, gov.uk, 19 June 2025, p 10

4 Pillar 1 – Security at Home

Pillar 1 overview

48. Pillar 1 of the National Security Strategy (NSS) concerns "Security at Home", setting out Government objectives to "defend our territory", "make the UK a harder target", and "build resilience to future threats".[69] It makes reference to a number of different domains through which domestic security is threatened and how this can be mitigated, including hostile "hybrid" activity (including against critical infrastructure) from foreign states, illegal migration "enabled by criminal gangs", and terrorism, including from "violence-fixated" individuals radicalised online.[70]

49. Given the issues of terrorism and extremism,[71] illegal migration,[72] and organised crime[73] have all recently been considered (or are currently being considered) by the Home Affairs Committee, this chapter focusses on the range of security vulnerabilities across critical national infrastructure (CNI).[74] The NSS highlights the need to bolster the defence of CNI within the context of increasing attacks against, for example, "undersea cables, energy pipelines, transportation and logistics hubs".[75] We examined this with particular reference to preparedness and resilience as outlined in the Resilience Action Plan[76] and associated strategies.

69 HM Government, National Security Strategy, June 2025, pp 21–28
70 HM Government, National Security Strategy, June 2025, p 21
71 Home Affairs Committee, Combatting New Forms of Extremism (accessed 25 February 2026)
72 Home Affairs Committee, Border security and irregular migration (accessed 25 February 2026)
73 Home Affairs Committee, The impact of serious organised crime on local neighbourhoods (accessed 25 February 2026)
74 Chemicals; Civil Nuclear; Communications; Defence; Emergency Services; Energy; Finance; Food; Government; Health; Space; Transport; Water – National Protective Security Authority, Critical National Infrastructure (accessed 25 February 2026)
75 HM Government, National Security Strategy, June 2025, p15; The International Institute for Strategic Studies (IISS) estimated (August 2025) that Russian hybrid-warfare activity across Europe jumped from fewer than 5 events in 2018 to over 30 in 2024: IISS, The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure, 18 August 2025, p3
76 The Resilience Action Plan provides additional detail on many of the measures the NSS describes in Pillar 1, specifically: improving the level of baseline resilience of the UK's critical national infrastructure; enabling a whole-of-society approach to resilience; and strengthening public sector resilience—HM Government, The UK Government Resilience Action Plan, 8 July 2025

50. In evidence, we heard of the need to:

- Bolster the resilience of critical national infrastructure, including that operated by private organisations;
- Ensure effective scrutiny of public sector preparedness plans; and
- Improve levels of public awareness and resilience to threats as part of the Government's ambition to have a 'whole-of-society' approach to security and resilience.

Protecting Critical National Infrastructure

51. Throughout our inquiry, stakeholders highlighted the need for the UK to deter hybrid attacks on CNI by, for example, "convincing adversaries that sustained coercion will be ineffective, costly, and overtaken by adaptation".[77] Air Commodore (retd) Blythe Crawford, Director of Tiberius Aerospace, told us the credibility of deterrence partly rests on "the ability to impose costs rapidly and proportionately" which, in turn, requires "attribution at speed".[78] This is in part dependent on whole-of-government integration, given that capabilities for responding to hybrid threats often "sit outside traditional defence acquisition yet depend on industrial capacity".[79]

52. We also heard that the Government may need to consider its definition of CNI. The National Preparedness Commission, for instance, raised concerns that it was unclear how far the planned Defence Readiness Bill[80] will extend the current definitions of CNI operators and suppliers and whether it would look to require larger companies to make Resilience Statements as part of their annual accounts.[81] The National Energy System Operator (NESO) told us it was working with the Government on a number of strategies relating to the security of CNI, including an Energy Resilience Strategy; Energy Security Strategy and Physical Security Strategy.[82]

53. We also heard of the importance of clarifying the expectations of private sector organisations involved in the protection of CNI, and what new requirements will be placed on them as part of efforts to shore up collective resilience. Suggested changes to requirements for private organisations with CNI responsibilities include:

77 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
78 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
79 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
80 Ministry of Defence, Strategic Defence Review, June 2025 p19
81 National Preparedness Commission (TNS0001)
82 National Energy System Operator (TNS0031)

- Requiring sectoral regulators to receive regular vulnerability assessments of CNI by operators, including stress testing;[83]
- Requiring larger companies to make a Resilience Statement covering how they address material risks, including cyber threats, as part of annual accounts;[84]
- Expanding the designation of what infrastructure is classed as CNI including, for example, digital identity verification providers;[85] and
- Mandating minimum security requirements to embed 'secure-by-design' and 'secure-by-default' principles[86] as well as minimum standards for physical and digital protection for facilities.[87]

Cyber security and resilience

54. On cyber resilience of CNI, witnesses highlighted points for the Government to consider during passage of the Cyber Security and Resilience (Network and Information Systems) Bill, which is currently making its way through Parliament, including:

- Balancing the enforcement approach of the regulatory regime with incentivising investment in cyber security and resilience;[88] and
- Clarifying expectations of private operators regarding managing digital security and resilience.[89]

Use of Reserves

55. The Strategic Defence Review (SDR) recommended that, as part of plans for Home Defence, UK Reserve Forces may be more involved in the protection of CNI in future, including "in the event of crisis or conflict."[90] In evidence, we heard that Estonia and Finland are looking at mobilisation plans for reserves, including "how significant the logistical effort will be in [a] conflict".[91] Captain (N) Juha Ravanti, Finnish Defence Attaché to the United Kingdom, told us that Finland currently has some 280,000 troops

83 The Centre for Long-Term Resilience (TNS0009)
84 National Preparedness Commission (TNS0001)
85 iProov (TNS0002)
86 NCC Group (TNS0012)
87 Thales UK Limited (TNS0027)
88 Thales UK Limited (TNS0027)
89 NCC Group (TNS0012)
90 Ministry of Defence, Strategic Defence Review, June 2025, p90
91 Q44

in its reserve and is considering taking on 20–30,000 more.[92] The UK, by comparison, had just under 32,000 Reserves as of October 2025,[93] many of whom report not feeling valued.[94]

56. As part of the Armed Forces Bill, also making its way through Parliament, the Government says it plans to expand the pool of reserves by increasing the maximum age limit for recall, enabling "seamless transfer between regular and reserve forces" and giving "the Secretary of State power to authorise recall for warlike operations".[95] However Mr David McFarland MBE, Associate Member of Lancaster University's Centre for War and Diplomacy, told us:

> Beyond identifying the Royal Navy as the lead in protecting subsurface critical infrastructure there is a lack of clarity on the requirement for the military to protect CNI.[96]

57. **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.

58. **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.

92 Q44
93 Ministry of Defence, Quarterly service personnel statistics: 1 October 2025, gov.uk (accessed 17 February 2026)
94 Ministry of Defence, Tri-service reserves continuous attitude survey 2025: main report, gov.uk (accessed 17 February 2026)
95 Ministry of Defence, Armed Forces Bill 2026, gov.uk (accessed 3 March 2026)
96 Mr David McFarland (TNS0003)

59. **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.

Scrutiny of public sector resilience

60. The UK Resilience Academy (UKRA) was established in April 2025,[97] to scrutinise preparedness plans for "whole-system civil emergencies", and to provide training "to all those across our society who play a vital role in our national resilience, in the light of gaps being identified in the Covid-19 Inquiry report".[98] In its Resilience Action Plan, the Government sets out a number of additional measures it is taking to further improve public resilience, including investments in flood defences, National Biosecurity Centres, new technology and infrastructure for telecommunications networks,[99] and measures to improve the work of Local Resilience Forums (LRFs).[100]

61. Steve Vincent, Strategic Manager at the West Midlands Local Resilience Forum, told us that UKRA is looking at professionalising crisis-response services within LRFs, including reviewing "the outcomes of flooding or a national power outage" and how food, warmth and key communications are maintained in such circumstances.[101]

Stakeholder concerns over UKRA and public sector resilience

62. The National Preparedness Commission expressed concerns that UKRA will not be placed on a statutory footing,[102] as had been recommended by the Covid-19 Inquiry.[103] Lord Harris of Haringey, Chair of the National Preparedness Commission, told us that while the role of UKRA will be "useful", given its non-statutory footing, it is also "not necessarily a substitute for a standing body with the expertise to look at the full range of issues … it does not solve the

97 Cabinet Office, UK Resilience Academy to help secure Britain's future with "generational upgrade" in emergency training, gov.uk (accessed 4 March 2026)
98 HM Government, National Security Strategy, June 2025, p 27
99 HM Government, The UK Government Resilience Action Plan, July 2025, p 10, p 34, p 40
100 HM Government, The UK Government Resilience Action Plan, July 2025, pp 35–39
101 Q52
102 National Preparedness Commission (TNS0001)
103 UK Covid-19 Inquiry, Module 1: The resilience and preparedness of the United Kingdom, 18 July 2024, p 161

systemic problem".[104] The Chancellor of the Duchy of Lancaster (CDL) told us that he was not concerned that UKRA is not on a statutory footing, but that he would keep this decision "under review".[105]

63. It is unclear how far, if at all, UKRA is looking at preparedness plans beyond flooding and power outages, or how far planning extends to Reasonable Worst Case Scenarios as set out in the National Risk Register.[106]

64. The National Preparedness Commission expressed concern that the way in which UKRA's convening role would be delivered was unclear. The Commission told us there is "no explicit statement of intent to draw on capacity elsewhere in the training ecosystem", such as universities, the National Defence Academy, the National Fire Training Academy or the British Red Cross.[107]

65. The Centre for Long-Term Resilience characterised the funding landscape for public resilience as "marked by opacity and inconsistency" saying that it is impossible to determine the true scale of new investment.[108] The Centre warned this may erode trust, credibility and scrutiny, as well as leading to uncertainty for private sector investors.[109]

66. **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.

67. **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.

104 Q39
105 Q122
106 HM Government, National Risk Register 2025 edition, 16 January 2025
107 National Preparedness Commission (TNS0001)
108 The Centre for Long-Term Resilience (TNS0009)
109 The Centre for Long-Term Resilience (TNS0009)

68. **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.

Public awareness and whole-of-society approach

Public awareness

69. The NSS acknowledges the need for "building greater public awareness of the threats we face", including from attempts by adversaries to "erode public trust through the spread of disinformation".[110] The SDR points to measures to improve "the connection between the UK Armed Forces and wider society" through public engagement days, work in schools, and expanding the Cadet Forces and the provision of Defence training.[111] The NSS, by comparison, is light on detail in terms of how the Government plans to build public awareness of the national security threats facing the UK.

70. Lord Harris, Chair of the National Preparedness Commission, discussed the need for greater public education and engagement to improve understanding of the importance of resilience measures and spending.[112] Consistent with the SDR recommendations to re-connect society with defence, the Estonian and Finnish Defence Attachés told us the importance of both being open with the public about how security threats are developing and increasing the media profile of the armed forces to improve the connection between civil society and defence.[113]

110 HM Government, National Security Strategy, June 2025, p 12, p 15
111 Ministry of Defence, Strategic Defence Review, June 2025, pp 87–88
112 Q37
113 Q38

Whole-of-society approach

71. As well as strengthening the UK's ability to deter and respond to threats to security and resilience, adopting a whole-of-society approach to resilience should enable the nation to better withstand a crisis during which business-as-usual communications, infrastructure and supply chains cannot be relied upon.[114]

72. The CDL acknowledged the need to "bring the public with us"[115] when it comes to resilience and security. He told us the public are anxious and "alive to what is happening to the world" but at the same time "probably … think that a lot of [these] things… are quite far away".[116] The CDL cited Government action aimed at improving public awareness, including through public statements; speeches by intelligence agency heads;[117] and increases in defence spending.[118] The CDL acknowledged, however, that the 'Prepare' webpage on the Government's website is not sufficient in and of itself to develop the whole-of-society approach:

> We set out lots of information on GOV.UK/prepare that supports people to think about, if the power goes out at home, what you might want to do in advance to be able to go about your lives while you are waiting for it to be switched back on. But am I convinced that everyone goes on GOV.UK/prepare to prepare? No, so we probably need to go a bit further than we currently do.[119]

73. In its response to the House of Commons Defence Committee's report on *The UK contribution to European Security*, the Government said that the Ministry of Defence had developed an internal "Joint Concept note designed to support decision-makers" regarding a national conversation on defence and security, adding that a public version would be available "shortly".[120] The Government re-iterated that the Cabinet Office has the "overall lead"

---

114 A submission from Air Cdre Blythe Crawford (Director at Tiberius Aerospace) noted that "[…] deterrence credibility depends not only on frontline force structure, but on whether adversaries believe the UK (and allies) can sustain operations…the ability to… continue to function under sustained pressure—particularly across energy, data, and communications." See Air Cdre Blythe Crawford (TNS0029)

115 Q114

116 Q117

117 See for example: Secret Intelligence Service (MI6) and FCDO, Speech by Blaise Metreweli, Chief of SIS, gov.uk (accessed 4 March 2026); Security Service (MI5), Director General Sir Ken McCallum gives threat update, gov.uk (accessed 4 March 2026)

118 Q117

119 Q117. This reflects issues we discussed at a private event we hosted in January 2026 on Russia. Key themes included the need for the Government to do more to guide the public on how to prepare for a crisis and to communicate how it is deterring Russia, as part of a broader national conversation. A summary of the event can be found in the annex to this report.

120 Defence Committee, Sixth Special Report of Session 2024–26, The UK contribution to European Security: Government Response, HC 1658, para 4

for “strategic direction for public-facing communications” on resilience and that work is “ongoing to develop further public communications strategies that support national security and civil defence objectives”.[121]

74. **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.

75. **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.

121 Defence Committee, Sixth Special Report of Session 2024–26, The UK contribution to European Security: Government Response, HC 1658, para 4

5 Pillar 2 – Strength Abroad

Pillar 2 overview

76. In this chapter, we consider the threats from abroad faced by the UK, and the Government's ambitions to bolster collective security through reinforcing existing alliances and developing new strategic relationships, as outlined in Pillar 2 of the National Security Strategy (NSS). The NSS and Strategic Defence Review (SDR) primarily focus on European/North Atlantic security as part of the adoption of a 'NATO First' (but not 'NATO only') approach to defence and security. These documents also discuss the Government's commitment to continue to "operate, sustain, and renew" the UK's nuclear deterrent, and an ambition to build strategic relationships with partners outside of the Euro-Atlantic region, in particular within the Indo-Pacific and the Middle East.[122]

77. First, we focus on the increasing security tensions brought about by great power competition between the United States (a longstanding ally with whom the UK's relationship is changing) and China (a geostrategic challenge which the Government must take seriously as it looks to reset its relationship with Beijing). We then consider Russia, as the greatest threat to UK security, followed by an examination of the Government's approach to China, before finally considering the future of European collective security and a developing nuclear picture. Overall, our evidence indicated a lack of preparation by the Government to account for diminishing confidence in US security guarantees in Europe, hard capability gaps within the UK and Europe, and the need for tougher deterrence concepts to impose real-world costs on Russian aggression. We finish the chapter by briefly considering the UK's role and relationships in regions beyond the Euro-Atlantic, in particular the Indo-Pacific and Middle East.

122 HM Government, National Security Strategy, June 2025, pp 29–40; Ministry of Defence, Strategic Defence Review, June 2025, pp 72–81

78. The rest of this chapter details findings, conclusions and recommendations for these aspects of Pillar 2 in turn. These should be understood within a broader, changing, global context that the Government must now navigate of:

- greater mistrust and higher tensions between nations;
- the re-assertion of great power competition over faith in multilateral institutions; and
- increased protectionism in economic policies on free trade, cooperation and development assistance.[123]

79. **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.

80. **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.

The threat from Russia

81. The SDR identifies Russia as the most acute threat to UK security, describing this threat as "immediate and pressing" through both conventional and hybrid capabilities.[124] This section will consider the threats Russia poses,

123 See for example: Politico, "Carney constructs a mega anti-Trump trade alliance", 12 February 2026; Carnegie Russia Eurasia Center, The Middle Power Moment (accessed 4 March 2026); Dr Roli Asthana (London School of Economics), Middle powers, UK, India and pivoting smarter (accessed 4 March 2026)

124 Ministry of Defence, Strategic Defence Review, June 2025, p 28

including Nuclear and conventional threats and hybrid and cyberattacks, as well as exploring how the UK can best deter and respond to continued Russian aggression.

Hybrid aggression

82. Expert witnesses to our inquiry agreed with the Government's assessment that Russia poses the most acute national security threat to the UK, citing in particular the use of hybrid tactics: sabotage, asymmetric attacks and cyberattacks.[125] Professor Michael Clarke, Distinguished Fellow at RUSI, described these threats as "much more challenging" than previously. He told us:

> Russian intelligence services […] work incredibly well with their own private sector. They do not initiate ransomware attacks, but they create the environment in which they encourage them and certainly do not object to them.[126]

83. The threat of political interference through hybrid means is of particular concern.[127] The Chancellor of the Duchy of Lancaster (CDL) told us that the ongoing Rycroft Review into foreign interference in UK politics will provide the Government with "suggestions" to take this issue forward.[128] The Representation of the People Bill currently going through Parliament[129] also represents an opportunity for the Government to put in place more robust measures to tackle foreign influence in political finance.[130]

Strategic stability and growing nuclear concern

84. There has been growing concern in recent years around the risk of nuclear escalation by Russia in light of comments made by the President Putin since the 2022 full-scale invasion of Ukraine.[131] While Rose Gottemoeller, former Under Secretary of State for Arms Control and International Security at the US State Department, described NATO's view of the likelihood of nuclear

125 Q3 [Lord Ricketts]; Q4 [Dr Rachel Ellehuss]
126 Q13; Q20
127 For further work the Committee is undertaking in this area, see: Joint Committee on the National Security Strategy, Defending Democracy (accessed 23 February 2026)
128 Ministry of Housing, Communities and Local Government, Independent review: countering foreign financial influence and interference in UK politics: Terms of Reference, gov.uk (accessed 4 March 2026). The review is due to report before the end of March 2026. See: Q122
129 Representation of the People Bill [as introduced], Bill 384 (2024–26)
130 Oral evidence taken on 9 February 2026, Q46, Q49, Q53, Q55
131 House of Commons Library, Russia's use of nuclear threats during the Ukraine conflict, Research Briefing 9825, 20 December 2024

weapons being used as "extremely remote",[132] investments in long-range precision strike systems and the modernisation of Russia's conventional warfighting capability in recent years, were highlighted as a risk.[133] So too was the increasing cooperation within 'CRINK'[134] which has supported Russia's war in Ukraine, although "does not truly represent an axis yet".[135]

Deterring Russian aggression

85. As we previously noted in our report on *Subsea telecommunications cables: resilience and crisis preparedness*, in addition to securing the resilience of society and critical infrastructure, the Government must also "be prepared to impose genuine costs for state-backed sabotage that go beyond public attribution".[136] Air Commodore (retd) Blythe Crawford said that, in addition to denial through resilience and attribution, the UK must also:

> be able to respond with graduated, reversible, and scalable effects, not only kinetic ones … cyber effects, electronic warfare, legal and regulatory actions, financial and trade measures, and exposure of malign activity.[137]

86. An example of imposing such costs would be the taking down of Russian shadow fleet vessels in co-ordination with allies.[138] As the Institute for the Study of War recently noted, "European countries appear to be cracking down against oil tankers associated with the shadow fleets of Russia and its allies".[139] Additionally, continued military and financial support for Ukraine (in part funded through money raised against sanctioned Russian sovereign assets) in its fight against Russia can be seen as part of the "increasing pressure" the UK and allies are looking to exert to deter Moscow from further aggression and to demonstrate collective NATO unity in response.[140]

---

132 Q61
133 Q54
134 China, Russia, Iran and North Korea
135 Q66
136 Joint Committee on the National Security Strategy, Subsea telecommunications cables: resilience and crisis preparedness, First Report of Session 2024–26, HC 723, p 2
137 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
138 According to the Government, the Russian shadow fleet "comprises ships engaged in illegal operations for the purposes of circumventing sanctions, evading compliance with safety or environmental regulations, avoiding insurance costs or engaging in other illegal activities." See Prime Minister's Office, 10 Downing Street and FCDO, The 'shadow fleet': a call to action, gov.uk, (accessed 6 March 2026)
139 Institute for the Study of War, Russian Offensive Campaign Assessment (accessed 4 March 2026)
140 HM Government, National Security Strategy, June 2025, pp 31–33. This reflects issues we discussed at a private event we hosted in January 2026 on Russia. Key themes included the need for the Government to impose greater diplomatic, economic and military costs on Russia. A summary of the event can be found in the annex to this report.

87. We also heard concerns regarding Russia's activity in the Arctic, and the impacts on the wider security of the region. While this was not a primary focus of this inquiry given concurrent work by the Defence Committee on the subject,[141] more detail can be found in the annex to this report.

88. **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.

89. **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.

The threat from China

90. The NSS characterises China as a "geostrategic challenge" rather than an acute hostile threat, as is the case with Russia. The UK's relationship with China demands trade-offs between opportunities for economic growth and risks to national security.[142] The NSS recognises this, outlining an ambition for a relationship with China which represents "pragmatic cooperation where it is in our national interest" while also having a "threat-driven" national security response, including the continued protection of the Hong

141 Defence Committee, Defence in the High North (accessed 23 March 2026)
142 HM Government, National Security Strategy, June 2025, p 39

Kong community in the UK from transnational repression.[143] This has been characterised elsewhere as the "three Cs" approach (compete; cooperate; challenge).[144] In January 2026, the Prime Minister's visit to China saw a new services partnership agreed, in addition to a relaxation of visa rules for UK citizens travelling to China.[145]

91. This section will consider the challenges posed by China, including: supply chain dependencies; political interference and strategic cooperation with Russia; and explore options for how the Government might best address these.

Supply chains

92. China is the major global player in supply chains upon which the UK is dependent, including in key economic areas. As the House of Commons Business and Trade Committee identified in its report on economic security, "China dominates the majority of the UK's critical mineral supply chains" and has tightened its rare earth export controls following the imposition of higher US tariffs in April 2025.[146] The Committee concluded that the UK is in this respect "significantly exposed to disruptions in their supply [with] considerable potential for adversaries to use this to their advantage".[147]

93. Isabel Hilton, founder of non-profit organisation China Dialogue and Senior Associate Fellow at RUSI, but appearing in a personal capacity, told us of the "potential security risks of anything that we do with China", including the importing of cheap low-carbon goods and technologies as part of the green transition, "which can then be weaponised" as well as the connection of such technologies with the UK's critical national infrastructure.[148] In its 2023–25 report, the Intelligence and Security Committee of Parliament (ISC) described China as targeting the UK and its interests "prolifically and aggressively" and that the UK is "playing catch-up … to understand and counter the threat."[149]

143 HM Government, National Security Strategy, June 2025, p 39
144 Chatham House, What the UK must get right in its China strategy, 8 July 2025, p 6
145 Prime Minister's Office, 10 Downing Street, Prime Minister unlocks new opportunities for British businesses in China, gov.uk (accessed 4 March 2026). The agreement will end "the requirement for travel [visas] under 30 days…bringing the UK into line with 50 other countries including France, Germany, Italy, Australia and Japan."
146 Business and Trade Committee, Eleventh Report of Session 2024–26, Toward a new doctrine for economic security, HC 835, para 48
147 Business and Trade Committee, Eleventh Report of Session 2024–26, Toward a new doctrine for economic security, HC 835, para 50
148 Q77
149 Intelligence and Security Committee of Parliament, Annual Report 2023–2025, HC 1544, paras 11–13

94. The Security Minister told us that the Government must have a "clear eyed approach to China". He told us:

> The public will understand that we do need to make the most of economic opportunities and areas like economic co-operation and climate change, but also on other important areas as well—whether that is narcotics trafficking, whether that is organised immigration crime, whether that is serious organised crime—it is entirely reasonable to engage in a way that is in our national interest […] But safeguarding our national security is always going to be a priority, and we will always make sure that we have got the right tools and the right resources in place to guard against that particular threat.[150]

95. Isabel Hilton also cited the need for greater convergence between the UK's approach to China and that of its allies in Europe, in particular on technological and supply chain risks. She told us that this should be actively explored and that we "should be prepared to bear [the] cost" of reducing dependencies on Chinese imports. Nigel Inkster, former Assistant Chief and Director of Operations at MI6, agreed that the Government should "start with the worst-case assumptions and work back from them".[151]

Interference and the Foreign Influence Registration Scheme

96. The UK's Foreign Influence Registration Scheme (FIRS) came into force in July 2025. The political tier of FIRS requires registration of arrangements to carry out political influence activities in the UK at the direction of any foreign power.[152]

97. Jonathan Hall KC, Independent Reviewer of Terrorism Legislation, told us there is "quite a strong case"[153] for specifying China under the enhanced tier of FIRS.[154] This would mean that individuals and entities would have to register any arrangement they have with China which involves a direction to carry out relevant activities in the UK.[155] Failure to register is a criminal offence which risks up to five years in prison and a fine (compared to

150 Q120
151 Q120
152 HM Government, FIRS public register, gov.uk (accessed 26 February 2026)
153 Q86
154 Joint Committee on the National Security Strategy, Second Report of Session 2024–26, Espionage cases and the Official Secrets Acts, HC 1414
155 The term "relevant activities", unless amended by the Secretary of State, includes all activities in the UK such as commercial activities, research activities and the provision of goods and services.

two years and a fine under the 'political influence' tier).[156] Additionally, Tim Law, former UK Defence Attaché in Beijing and Director at UK-China Transparency, said that FIRS is currently "too weak on China" and that this should be reviewed on a continual basis.[157]

98. The Security Minister acknowledged these concerns: he told us that specifying China under the enhanced tier may be a "useful capability" but that it is still "relatively early days" for FIRS, and the Government is reviewing how specification under this tier is working with regards to Russia and Iran.

99. Interference also occurs within academia. For example, in 2024 China reportedly "waged a campaign of harassment and intimidation directed at [Sheffield Hallam University] to get it to shut down sensitive research into alleged human rights abuses",[158] and concerns were raised that universities did not know to whom they should report instances of interference.[159] In February, it was reported that the Security Minister and the Minister for Skills told University Vice-Chancellors that threats of foreign interference across academia should be reported directly to the Government and security services, and that £3m would be spent on "on measures including a new secure platform" for university leaders to report "suspicious approaches or interference".[160] The Government also provides guidance on guarding against foreign interference in higher education on gov.uk.[161]

New Chinese embassy

100. The Government approved the construction of a new Chinese embassy in London in January 2026, despite some commentators expressing concerns over potential security risks.[162] The Security Minister told us that this decision had been made based on the advantages of drawing down the current number of Chinese diplomatic sites from seven to one, and that he was "satisfied we have got appropriate mitigations" to deal with any security risks from the site.[163] In its response to the Government's decision, the ISC acknowledged that national security concerns arising from the embassy

156 Home Office, Factsheet: What is the Foreign Influence Registration Scheme, gov.uk (accessed 6 March 2026)
157 Tim Law (TNS0005)
158 BBC News, "China intimidated UK university to ditch human rights research, documents show", 3 November 2025
159 Q88
160 BBC News, "Universities told to report foreign interference on campus to MI5", 9 February 2026
161 Department for Education, Protecting UK higher education from foreign interference, gov.uk (accessed 6 March 2026)
162 BBC News, "UK approves plans for Chinese mega-embassy", 20 January 2026
163 Q121

could be "satisfactorily mitigated", but stated it was not convinced that the Government had "managed to reconcile internally that China can be both an economic partner and a national security threat".[164]

Strategic cooperation with Russia

101. The NSS acknowledges that China and Russia increasingly engage in strategic and opportunistic cooperation.[165] As Air Marshal (retd) Edward Stringer, Senior Fellow at Policy Exchange, told the House of Commons Defence Committee in February 2026, China is "discreetly" supporting Russian aggression in Ukraine by, for example, building railway supply lines to drone factories:

> About 60% of what is keeping the Russian war effort and economy going comes from China … Russia can only maintain this war because China is essentially bankrolling it.[166]

102. It has also been reported that China has supported Russia's war effort by:

- sharing intelligence gathered through reconnaissance flights;[167]
- trading technology and advanced equipment, including specialised manufacturing for warheads for hypersonic missiles[168] and exports of drone parts such as fibre-optic cables and lithium-ion batteries;[169] and
- not intervening in North Korea's military involvement in the war despite its significant influence over its neighbour and ally.[170]

---

164 Intelligence and Security Committee of Parliament, Press Notice, 20 January 2026

165 The National Security Strategy notes that there is "evidence of countries like Russia, China, Iran and North Korea cooperating across theatres—sometimes opportunistically and sometimes by deepening strategic ties". See HM Government, National Security Strategy, June 2025, p 35

166 Oral evidence taken by the Defence Committee on 3 February 2026, Q11. See also: Carnegie Politika, Can China Compensate Russia's Losses on the European Gas Market? (accessed 4 March 2026)

167 Council on Foreign Relations, China in Russia and Ukraine: October 2025 (accessed 26 February 2026)

168 U.S.-China Economic and Security Review Commission, China's Position on Russia's Invasion of Ukraine (accessed 26 February 2026)

169 Council on Foreign Relations, China in Russia and Ukraine: October 2025 (accessed 26 February 2026). The Atlantic Council reported that while Ukraine has also sourced drone components from China during the war, "export volumes to Russia now dwarf deliveries of key component categories to Ukraine"—see Atlantic Council, US voices concern over Chinese support for Russia's Ukraine invasion (accessed 26 February 2026)

170 French Institute of International Relations, The China-Russia Partnership and the Ukraine War: Aligned but not allied (accessed 26 February 2026)

Emerging challenges

103. In addition to the above, experts have also pointed to emerging challenges from China which the UK may have to grapple with at greater scale in the near future. These include:

- espionage cases within Parliament which we have previously reported on,[171] and new potential cases of which emerged in March 2026;[172]
- transnational repression, including violence against and intimidation of UK-based Hong Kong citizens.[173] Lord Patten highlighted "not all" UK universities protect Hong Kong students from Chinese interference "as effectively as they should";[174] and
- the potential for AI-enabled misinformation and data exploitation through platforms such as DeepSeek.[175] Dr Lorna Waddington, Associate Professor of International History at the University of Leeds, said that DeepSeek "demonstrates how state-controlled AI can embed systematic biases serving geopolitical interests."[176]

104. **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.

171 Joint Committee on the National Security Strategy, Second Report of Session 2024–26, Espionage cases and the Official Secrets Acts, HC 1414

172 BBC News, "MP's husband and two political advisers bailed after arrests over alleged China spying", 5 March 2026

173 BBC News, "The A-level student who became an enemy of the Chinese state", 16 February 2025; Politico, "UK summons senior Chinese diplomat over violent attack at Manchester consulate", 18 October 2022; The Guardian, "Hong Kong protestors allegedly attacked by Chinese activists in Southampton", 12 June 2023

174 Q78

175 CSIS, Delving into the Dangers of DeepSeek (accessed 4 March 2026); University of Bristol, New AI app DeepSeek poses 'severe' safety risk, according to new research (accessed 4 March 2026)

176 Dr Waddington (Associate Professor at University of Leeds) (TNS0013)

105. **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.

The transatlantic alliance and UK security

106. The NSS describes the US as the UK's "most important defence and security ally", citing mutual commitment to NATO, intelligence and nuclear sharing and interoperability of armed forces.[177] There have been concerns expressed among stakeholders and experts, however, over whether the UK is doing enough to adjust to a geostrategic reality where the US has a much reduced security presence in Europe, and to mitigate the potential risks posed by interdependencies between UK and US intelligence and military capabilities. These aspects will be considered in turn in this section.

Changing geostrategic reality

107. Concerns over misalignment between UK and European interests, and those of the US, have intensified since the publication of the US's National Security Strategy in December 2025 and its National Defense Strategy in January 2026,[178] the first of which warned of "civilizational erasure" in Europe and the desire of the United States to "help Europe correct its current trajectory."[179] This was followed by repeated comments by President Trump on 'acquiring' Greenland,[180] to which Danish Prime Minister Mette Frederiksen responded by saying that an attack by the US on Greenland would mean that "everything stops, including NATO and thus the security that has been established since the end of the Second World War."[181]

177 HM Government, National Security Strategy, June 2025, pp 33–34
178 US Department of War, 2026 National Defense Strategy, 23 January 2026
179 The White House, National Security Strategy of the United States of America, November 2025, pp 25–26
180 House of Commons Library, President Trump and Greenland: Frequently asked questions, Research Briefing, 23 January 2026
181 Politico, "NATO is done if Trump invades Greenland, Danish PM warns", 5 January 2026

108. Tensions remain high between NATO allies over, for example, the sovereignty of Greenland;[182] the strategic position of the Arctic[183] and attitudes to the US-Israeli air strikes against Iran.[184] The High North deserves particular attention, given the pace of environmental change and deepening international competition over access to resources and security-relevant locations.[185] We noted that the UK's rhetoric on Arctic security has not been met with commensurate military and scientific resource commitments to secure its interests.[186]

109. The Foreign Secretary told the House of Commons Foreign Affairs Committee in December 2025 that "there are also areas where … we take a different view" to the US's approach to security issues. However, she added that areas of the US's National Security Strategy represent a "shared vision" with the UK,[187] and that there was "continued strong support from the US for NATO".[188]

110. The Chancellor of the Duchy of Lancaster (CDL) told us that the Government did not share Canadian Prime Minister Mark Carney's view that "middle power" liberal democracies need to move on from the post-war global security settlement.[189] The CDL added that the UK has "frank conversations" where it disagrees with the US and that the UK Government is in agreement on the need for "Europe collectively … to increase its defence capabilities."[190]

111. In response to the House of Commons Defence Committee's report on European security, the Government said that it would "continue to identify opportunities for further defence industrial cooperation with the EU as we jointly implement the Security and Defence Partnership" and that it is "actively partnering" to "leverage the strengths of British industry in delivering European security", citing "major agreements" with Norway, Türkiye, Germany and France.[191]

---

182 LSE Blogs, Trump's Greenland threats placed US allies and military in an impossible position (accessed 4 March 2026)

183 NATO, NATO's activities in the Arctic and High North (accessed February 2026) – the Defence Committee are currently considering this issue in its inquiry into Defence in the High North

184 The Independent, "Trump hits out at Starmer over Iran: 'This is not Winston Churchill we're dealing with'", 4 March 2026

185 See Annex 1.

186 Please see Annex 1 for more detail on the changing security dynamics in the Arctic

187 Oral evidence taken by the Foreign Affairs Committee on 16 December 2025, Q478

188 Oral evidence taken by the Foreign Affairs Committee on 16 December 2025, Q480

189 Q129

190 Q125

191 Defence Committee, Sixth Special Report of Session 2024–26, The UK contribution to European Security: Government Response, HC 1658, para 3

Risk of interdependencies

112. There is concern among stakeholders and experts that the closeness of the US-UK defence and security partnership has resulted in interdependencies for the UK that could pose challenges for security and resilience in the coming years. Civil society organisation Rethinking Security told us the NSS "fails to analyse or account for … the UK's continued acute dependence on the United States".[192] Others flagged issues of dependence in the context of conflict, with the Council on Geostrategy warning "the US may not be able or willing to provide NATO's ultimate backstop" in the event of nuclear escalation with Russia,[193] and Lieutenant Colonel (retd) Haydn Gaukroger cited possible reliance on the US "for the supply of key drone capabilities/technologies".[194]

113. Despite this, we heard that deep strategic collaboration with the US will continue to be necessary. Grace Cassy, external reviewer for the SDR, told us the US is "still a hugely important partner" in terms of technological development and shared capability.[195] Dr Rachel Ellehuus, Director General of RUSI and former US Secretary of Defense Representative in Europe, judged that the UK has further "room for partnership" with both the US and Europe; for example, in cloud systems.[196] Lord Peter Ricketts, then Chair of the House of Lords European Affairs Committee and former National Security Adviser, told us the UK and the US continue to have "very similar interests" across national security policy even if they "do not map on each other directly",[197] while Professor Michael Clarke concluded that "we must of course hold on to our relationship with the United States", even as this relationship changes.[198]

114. In early 2026, some expert opinion diverged from this view given the actions of the US administration. Bronwen Maddox, Director and Chief Executive of Chatham House, for example, suggested the UK (and Europe)-US relationship has now fundamentally changed[199] while Nick Witney, Senior Policy Fellow at the European Council on Foreign Relations, said that the UK would benefit by actively working to reduce its dependencies on the US.[200]

---

192 Rethinking Security (TNS0015)
193 Council on Geostrategy (TNS0025)
194 Haydn Gaukroger (Head of Capability Development at Syos Aerospace) (TNS0030)
195 Q20
196 Q7
197 Q6
198 Q20
199 Chatham House, The Director's Annual Lecture 2026, 13 January 2026
200 European Council on Foreign Relations, Escaping the special relationship: How Britain can leave its dangerous dependency on Trump's America, 10 February 2026. This reflects issues we discussed at a private event we hosted in January 2026 on Russia. Key themes included potential measures to offset strategic reliance on the US. A summary of the event can be found in the Annex to this report.

115. The CDL told us the UK continues to "collaborate very closely every day" with the US, saying that there is "nothing wrong with the US having a view of its own interests" and did not accept the premise of "de-risking" the relationship.[201] The Government has said it is deepening its defence relationship with the US through, for example, making progress towards a 'Technology Prosperity Deal'[202] and an 'Economic Prosperity Deal'.[203]

116. In addition to cooperation through NATO, the UK has a close, albeit changing, bilateral relationship with the US that may have consequences for its national security. These include:

- the UK's dependence on the US for maintenance of its Trident missiles;[204]
- intelligence sharing arrangements, most notably through Five Eyes;[205]
- a number of partnerships to deliver conventional capabilities, such as the F-35 program;[206]
- the AUKUS partnership, to deliver new, nuclear-powered, attack submarines and other advanced military technology;[207] and
- special operations forces.[208]

117. As reflected in President Trump's repeated comments on the merits of the UK's decision to transfer sovereignty of the Chagos Archipelago to Mauritius,[209] and the willingness of the US administration to use tools such as tariffs against traditional allies where they perceive there is a conflict with US interests,[210] there are demonstrable areas of tension in the UK-US relationship that may compromise the reliability of these dependencies in the near future.

---

201 Q128

202 Prime Minister's Office, 10 Downing Street, Memorandum of Understanding between the Government of the United States of America and the United Kingdom of Great Britain and Northern Ireland regarding the Technology Prosperity Deal, gov.uk, 18 September 2025

203 Department for Business and Trade, UK-US Economic Prosperity Deal (EPD), gov.uk (accessed 17 February 2026)

204 Q59

205 Q20 [Professor Michael Clarke]

206 Center for Strategic and International Studies, Making the U.S.-UK Special Relationship Fit for Purpose, 15 July 2025

207 Ministry of Defence, UK submarine arrives in Australia in AUKUS partnership first, gov.uk, 23 February 2026

208 Center for Strategic and International Studies, Making the U.S.-UK Special Relationship Fit for Purpose, 15 July 2025

209 The Telegraph, Britain faces paying billions if Trump collapses Chagos deal, 22 February 2026

210 Peterson Institute for International Economics, US-China Trade War Tariffs: An Up-to-Date Chart (accessed 24 February 2026)

118. **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).

119. **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.

120. **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.

International Partnerships

121. The NSS makes clear the Government's ambitions to develop strategic partnerships with countries in the Indo-Pacific and Middle East, and that NATO considers the security of the Euro-Atlantic and the Indo-Pacific as "inextricably linked".[211] We heard of the potential opportunities to be gained from the UK developing its strategic relationships with the Gulf countries, India and other partners in Asia (such as Japan, through the Global Combat Air Programme).

211 HM Government, National Security Strategy, June 2025, p 10

122. Will Todman, Senior Fellow in the Middle East Program at the Center for Strategic and International Studies, told us on 20 October 2025 that the UK has an important role to play in the Middle East's security.[212] He added that a free trade agreement between the UK and the Gulf Cooperation Council (GCC)—under negotiation—would "spark a lot of deeper technology partnerships."[213]

123. Asoke Mukerji, former Permanent Representative of India to the UN, said that the Government could engage more with India in its planning for region security through SAGAR (Security and Growth for All in the Region).[214] The Lords International Agreements Committee concluded in February 2026 that the UK's new Free Trade Agreement with India marks a "significant achievement",[215] given the uncertain environment for international commerce, with trade "increasingly embedded in geographical strategy."[216]

124. The AUKUS and GCAP projects are two examples of existing capability programmes that are designed to strengthen the UK's partnerships in the Indo-Pacific, which may provide lessons for other programmes the UK is seeking to develop with global partners.[217]

125. **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.

126. **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.

212 Q70
213 Q72
214 Q67
215 House of Lords International Agreements Committee, Fourteenth Report of Session 2024–26, Scrutiny of international agreements: UK-India Comprehensive Economic and Trade Agreement, HL Paper 253, para 11
216 House of Lords International Agreements Committee, Fourteenth Report of Session 2024–26, Scrutiny of international agreements: UK-India Comprehensive Economic and Trade Agreement, HL Paper 253, para 21
217 On AUKUS, see Q110 [Sophia Gaston], as well as evidence gathered by the Defence Committee via its ongoing inquiry: Defence Committee, AUKUS [accessed 23 March 2026]

Changing nuclear context

127. The NSS describes the UK's independent nuclear deterrent as the "most important national capability" and commits to "ensuring a continuous at-sea presence, building new submarines and upgrading the fleet" as well as investments in the sovereign warhead programme (£15bn) and the Dreadnought submarine programme (£31bn).[218]

128. As Rose Gottemoeller, former Under Secretary of State (US) for Arms Control and International Security and former Deputy Secretary of NATO, indicated, the UK has "independent command and control decision-making" over its deterrent, "with nuclear use decisions belonging very much to the Prime Minister".[219] However, the UK relies on the US to conduct maintenance of its Trident missiles "every few years", and "also purchases the aeroshells required for producing nuclear warheads from the US".[220]

129. According to the SDR, the global non-proliferation and disarmament regime is "now under strain".[221] It notes that, with the expiry of the New Strategic Arms Reduction Treaty (New START) on 4 February 2026, "the future of strategic arms control … does not look promising", given the "absence of willing partners in Moscow and Beijing".[222] The SDR stresses the need for continued UK leadership within the Non-Proliferation Treaty (NPT) and notes that by sustaining the UK's own deterrent, this will "assure Allies that they do not need nuclear weapons of their own".[223]

European nuclear posture

130. Attempts to reassure Allies in this respect include the signing of the Northwood Declaration between the UK and France in July 2025, aimed at deepening nuclear cooperation and coordination through the establishment of a Nuclear Steering Group to "coordinate across nuclear policy, capabilities and operations" as well as reaffirming "full support" for the Treaty on the non-proliferation of nuclear weapons".[224]

---

218 HM Government, National Security Strategy, June 2025, p 42

219 Q58. The SDR notes that the UK "would consider using nuclear weapons only in extreme circumstances of self-defence, including the defence of NATO Allies." See Ministry of Defence, Strategic Defence Review, p 98

220 Chatham House (Dr Marion Messmer and Olivia O'Sullivan), The UK's nuclear deterrent relies on US support – but there are no other easy alternatives, 24 March 2025

221 Ministry of Defence, Strategic Defence Review, p 100

222 Ministry of Defence, Strategic Defence Review, pp 100–102

223 Ministry of Defence, Strategic Defence Review, p 100

224 Prime Minister's Office, 10 Downing Street, Northwood Declaration: 10 July 2025 (UK-France joint nuclear statement), gov.uk, 10 July 2025

131. In the context of increasing threats from Russia around the use of nuclear weapons, there have been calls from stakeholders for a further strengthening of NATO's nuclear arrangements, including:

- Expanding the presence of US missile systems in Europe;[225]
- Extending the US nuclear-sharing arrangements to other NATO Allies; and
- Extending France's nuclear umbrella to protect other European states[226]—although commentators have suggested the Northwood Declaration represents a signal that France (and the UK) "will offer a form of joint protection to Europe".[227]

132. Discussions at the 2026 Munich Security Conference furthered this discussion, including on the need to re-assess the UK and France's nuclear posture, such as considering of the possibility of "strengthening the role of British and French nuclear forces in European deterrence."[228]

133. Rose Goettemoeller told us that, with regards to managing nuclear tensions, the NSS "pushes in [the right] direction but … We have to make some tough decisions about whether we try to control the nuclear bomb or let it run free".[229] She added that the UK, US and France "should be looking for ways to reassure our allies and partners so that friendly proliferation … does not become a trend",[230] and that efforts should be made to try and bolster existing non-proliferation regimes, for example by ensuring that new nuclear reactors are "proliferation-resistant".[231]

134. Dr Marion Messmer, Senior Research Fellow at RUSI, discussed the value of the UK's nuclear deterrent in NATO, and the continued importance of "showing that NATO joined-up European deterrence thinking is at the forefront of UK thought" when it comes to defending against Russian aggression.[232] Dr Messmer flagged concerns with the state of the

225 Atlantic Council, To deter Russia, NATO must adapt its nuclear sharing program, 30 July 2024
226 Chatham House, France should join NATO's nuclear sharing arrangements to strengthen European deterrence, 12 March 2025
227 IISS, The Northwood Declaration: UK-France nuclear cooperation and a new European strategic backstop, August 2025. See also: Atlantic Council, Reading between the lines of the new France-UK nuclear entente, 16 July 2025; French Institute of International Relations, How should Britain and France cooperate to realise the Northwood Declaration?, 18 July 2025
228 Munich Security Conference 2026—Report of the European Nuclear Study Group, Mind the Deterrence Gap: Assessing Europe's Nuclear Options, February 2026; Bulletin of the Atomic Scientists, In Munich, Europe tries to strike a balance: "We need a more European NATO", 12 February 2026
229 Q54
230 Q60
231 Q60
232 Q57

modernisation of the UK's nuclear capabilities including the "failed Trident test in February 2024", Vanguard submarines "returning to port with visible damage", and delays to the Dreadnought and warhead replacement programmes, saying that "we know that shipyards are facing challenges".[233]

135. **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.

136. **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.

233 Q57

6 Pillar 3 – Sovereign Capabilities

Pillar 3 overview

137. Pillar 3 of the National Security Strategy (NSS) acknowledges the need to build more sovereign capabilities in critical areas to secure the UK's future national security and international competitiveness.[234]

138. In this chapter, we consider how sovereign capabilities are defined; which sovereign capabilities should be pursued and to what extent; and how to revitalise the defence industrial base so that it can support in the pursuit of these capabilities.

Defining sovereign capabilities

139. The NSS does not provide the Government's definition of the term 'sovereign'. In general, it can be understood to mean the ability of a country to "autonomously develop, sustain and control critical technologies, capabilities and supply chains vital to its military strength and strategic autonomy."[235]

140. Industry stakeholders highlighted the ambiguous definitions of the term 'sovereign'. ADS Group stated that, while the NSS rightly articulates the need to "identify, nurture and protect… sovereign capabilities", it does not provide further detail on which capabilities will be owned outright, and those where access will be dependent on collaboration with partners.[236] To the Council on Geostrategy, a definition must take into account that "complete 'end-to-end' sovereignty" is "realistically near impossible".[237]

141. Professor Sir Anthony Finkelstein, former Chief Scientific Adviser for National Security, suggested that the sovereignty definition may need to be a "separately commissioned piece of associated analytic work" to provide "much finer-grain, much more intelligence-informed assessments framed

234 HM Government, National Security Strategy, June 2025, p 41
235 Advance (ADS), Prioritising sovereign capability, 17 April 2024
236 ADS Group (TNS0007)
237 Council on Geostrategy (TNS0025)

around the competitive setting."[238] Professor Sir Nigel Shadbolt, Executive Chair and Co-Founder of the Open Data Institute, added that a "crisper view" of sovereign capabilities "could serve us" and that, in the realm of AI, sovereignty could be understood to mean the ability to develop, host, understand, test and govern systems.[239] He also stressed the need for an "organised dialogue" between the private sector, academic institutions, regulators and Government to better define sovereign capabilities.[240]

142. The House of Commons Business and Trade Committee previously wrote to the Government requesting further clarity over the Government's ambitions to develop sovereign capabilities as part of the Defence Industrial Strategy.[241] The subsequently published Defence Industrial Strategy discusses the need to develop sovereign capabilities "by strengthening the defence sectors essential for national security and supply chain resilience" but fails to provide a definition.[242]

143. The Chancellor of the Duchy of Lancaster (CDL) confirmed to us that the Government does not have an agreed, written definition of what a sovereign capability is.[243] He told us sovereignty related to having "skills, capabilities and control over key infrastructure assets" and discussed upgrading IT systems within Whitehall through the Shared Services Program as part of this.[244] He added that, while the UK may not be able to achieve "end to end" sovereignty, "there are definitely parts of the value chain where we have great capabilities."[245]

144. The CDL told us he was "satisfied" that the Government was undertaking a lot of activity to meet challenges related to sovereign capabilities, including work in the Department for Business and Trade on supply chains and within the Cabinet Office for screening foreign investment into the UK as part of decisions under the National Security and Investment Act.[246] The Government has acknowledged the need to develop resilient supply

238 Q98
239 Q98
240 Q98
241 Letter from the Chair of the Business and Trade Committee to the Secretary of State for Business and Trade and the Secretary of State for Defence regarding the Defence Industrial Strategy, 18 June 2025
242 Ministry of Defence, Defence Industrial Strategy 2025: Making Defence an Engine for Growth, 8 September 2025, p 23
243 Q130
244 Q124
245 Q124
246 Q131

chains in aid of improving the UK's sovereign capabilities through additional strategies such as its Defence Industrial Strategy[247] and Critical Minerals Strategy.[248]

Which capabilities to prioritise?

145. Sovereign capabilities which witnesses to our inquiry indicated would be important to pursue and maintain include:

a. Military capabilities for effective deterrence, such as:

i) Independent nuclear deterrent, given this is "central to credible deterrence", including warhead and platform, but also "command, control, communications, sustainment, and safety assurance";[249]

ii) AI, including autonomous weapons systems[250] and 'adversarial' AI;[251] and

iii) In-theatre capabilities, including drones and the "education, regulation, test and evaluation facilities" for their development.[252]

b. Capabilities for ensuring national resilience in functions which underpin defence capabilities and critical national industries, such as steel manufacturing;[253] and

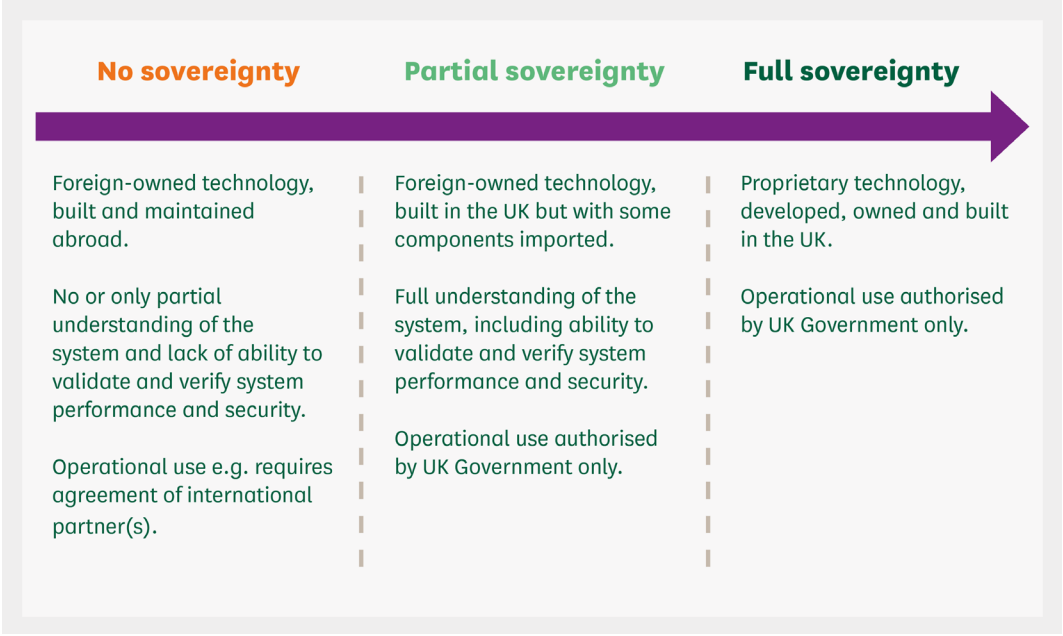
c. Capabilities vital to ensuring the continuation of critical and military operations in a warfighting scenario, such as communications networks,[254] munitions,[255] data assets and infrastructure and energy supply.[256]

247 Ministry of Defence, Defence Industrial Strategy 2025: Making Defence an Engine for Growth, gov.uk, 8 September 2025
248 Department for Business and Trade, UK Critical Minerals Strategy, gov.uk, 22 November 2025
249 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
250 Q106 [Lieutenant Colonel (retd) Haydn Gaukroger]
251 Q100 [Professor Sir Anthony Finkelstein] and Q106 [Air Commodore (retd) Blythe Crawford]—"where essentially two autonomous agents teach and train each other to develop new capability…we are world-leading in this regard, and we should be making more of it."
252 Haydn Gaukroger (Head of Capability Development at Syos Aerospace) (TNS0030)
253 Q107 [Sophia Gaston]
254 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
255 Thales UK Limited (TNS0027)
256 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)

Levels of sovereignty

146. In addition to identifying specific areas of technology to prioritise for sovereignty, Professor Finkelstein told us that determining the baseline sovereignty requirements for these technologies needs to be derived from a "threat scenarios" approach, adding that the Government should focus on having "minimum scientific technical understanding" so that it can "act as a smart customer" and "assure supply chains".[257] Professor Shadbolt added that, where systems have been procured from overseas, sovereignty also concerned the ability to "validate and verify complex systems" in terms of their security and performance. Air Commodore (retd) Blythe Crawford elaborated on this, telling us it is important to be clear on what capabilities need to be "purest sovereign" and which the UK can afford "to collaborate on with allies and partners".[258] A conceptualisation of these hypothetical levels of sovereignty can be seen in Figure 3.

Figure 3: Hypothetical levels of sovereignty



NB: Figure has been produced as part of analysis of evidence received to the inquiry; it does not necessarily reflect Government language or conceptualisation.

147. Air Commodore (retd) Crawford said that the Government needs to establish a sovereignty framework to distinguish between capabilities where there is a need for "assured national control" and those where interdependence is acceptable or beneficial. He said this was necessary as capability partnerships can create a "strategic veto" if, for example,

257 Q97
258 Q108

components, software updates, munitions or support arrangements are "delayed or denied through third-party permissions at precisely the moment they are needed".[259] Such a framework, he argued, would allow the UK to guard against "situations in which it possesses the platform but not the ongoing authority, data, or permissions required to generate effect".[260]

148. Sophia Gaston, Visiting Fellow, Department of War Studies at King's College London and Founder and Lead of the AUKUS Industry Forum, told us that "a much more active, interventionist state that is willing pick winners" was needed:

> If we want to have a laser focus on sovereign capability then we need to be willing to double down in areas of strength and make hard choices in that respect.[261]

UK strengths and skills

149. Witnesses to this inquiry highlighted that the Government will need to do more to maintain and bolster the skills the UK will need for achieving sovereignty in key areas, particularly AI. Professor Finkelstein spoke of the importance of understanding where skills gaps lie, as currently, "we just do not have an understanding of where we have skills shortages" and that "erosion in [the] underlying skills base is slow but ultimately more dangerous than crisis shocks".[262] techUK also highlighted skills shortages across both emerging technologies and traditional trades relevant for developing sovereign capabilities.[263]

150. Witnesses suggested a number of measures to help address skills shortages, including the National Computing Centre (NCC) Group, which called for a national programme of cyber skills, including investment in infrastructure for regional training providers and employer incentives for graduate-level hiring.[264] Additionally, on AI, Professor Shadbolt told us that while there is a "supply of talent" coming from universities, industry can be "somewhat extractive" and "graduates could well do with more time in the lab to develop … skills."[265]

259 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
260 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
261 Q107
262 Q97
263 techUK, TNS0020
264 NCC Group (TNS0012)
265 Q100

151. **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.

152. **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 utilised.

153. **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.

154. **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.

Defence industrial base

155. Stakeholders were clear about the need to improve the state of the UK's defence-industrial base in order to pursue sovereignty of key capabilities. Specifically, we heard evidence that there is a need for the Government to do more to identify capability gaps within the defence industrial base;

to provide greater clarity over funding allocations through the Defence Investment Plan; and to provide more scale-up support for Small and Medium-sized Enterprises (SMEs) vulnerable to acquisition.

Identifying gaps in the base

156. Defence contractor Thales UK Limited described a situation whereby the UK has "good capacity for assembly of final products" but lacks "immediate component production capacity".[266] Air Commodore (retd) Blythe Crawford suggested the Government conduct a "structured gap analysis" of the UK's industrial base to identify which gaps could be mitigated through allies and areas where there is a need to invest in onshoring capability.[267]

157. As a specific example, Lieutenant Colonel (retd) Haydn Gaukroger, Head of Capability Development at Syos Aerospace, told us of the issues he faced in sourcing capabilities as the former director for the UK drone programme for Ukraine:

> We found that pretty challenging across a whole range of different areas […] the availability of propulsion systems, motors, compute […] Finding sovereign sources of those kinds of capabilities was incredibly hard.[268]

158. The NSS states an ambition to "rebuild our core defence industrial base".[269] The Government has made a number of commitments regarding the revitalisation of the UK's defence-industrial base, primarily through its Defence Industrial Strategy, where it outlines measures to invest in regional defence-based growth, including through innovation and "high tech companies"; improve the defence skills base; offer new contracting and exporting opportunities for defence SMEs and conduct regular wargames with industry.[270] It adds that the Defence Investment Plan (DIP) will "outline our investment priorities".[271]

Lack of clarity over funding priorities

159. The Government has not yet published the DIP. Representatives from the defence, security and resilience industries argued that the Government has therefore not yet indicated how funding will be allocated across

266 Thales UK Limited (TNS0027)
267 Air Cdre Blythe Crawford (Director at Tiberius Aerospace) (TNS0029)
268 Q105
269 HM Government, National Security Strategy, June 2025, p 41
270 Ministry of Defence, The UK's Modern Industrial Strategy—Defence Industrial Strategy, gov.uk, 8 September 2025
271 Ministry of Defence, The UK's Modern Industrial Strategy—Defence Industrial Strategy, gov.uk, 8 September 2025, p 11

the sector to set expectations for firms, or how much of this will be for reviving the defence-industrial base versus building resilience for critical infrastructure.[272] Lieutenant Colonel (retd) Haydn Gaukroger said that the Government must be clear about the need to identify areas of weakness within the defence industrial base and work to incentivise companies to help fill these gaps.[273]

160. Industry bodies ADS Group and techUK cited this lack of clarity impacting the ability of firms to plan research and development spending in a way that prioritises the most important sovereign technologies.[274] For SMEs in particular, this could contribute to their vulnerability to acquisition by foreign investors. These bodies and companies such as Northrop Grumman called for the DIP to provide greater clarity on spending allocation and (sovereign) capability gaps.[275] Thales UK Limited said there also needed to be clarity on the "expected burden" the Government envisions on private organisations paying for resilience investment, arguing that there is often "a strong conflict between commercial profitability" and this kind of spending.[276]

Challenges to SMEs scaling up

161. Challenges for UK businesses looking to scale up were also identified. Sophia Gaston said that, while the UK is strong in generating start-ups, "we do not allow anything to move from the 'S' to the 'M' in 'SME'", leaving companies that could otherwise contribute to the development of the defence industrial base (and sovereign capabilities) vulnerable to acquisition.[277] This issue was also highlighted by the defence and security company, Programify, which said that a lack of structural support for SMEs leaves independent commercialisation as the only viable path, which "isolates capability from government oversight until much later".[278]

162. As of 12 January 2026, the Government said that it is "working flat out to finalise the DIP, which will be published as soon as possible".[279] This was followed by a statement in the House of Lords Chamber by Baroness Chapman that the plan "should be published when it is ready and we should not be rushed into doing things before that".[280] In January 2026, the CDL told us that he was conscious of the fact that the DIP is "late" but this is because

272 Thales UK Limited (TNS0027); ADS Group (TNS0007); Northrop Grumman UK (TNS0018); techUK (TNS0020)
273 Q107
274 ADS Group (TNS0007); techUK (TNS0020)
275 Northrop Grumman UK (TNS0018)
276 Thales UK Limited (TNS0027)
277 Q107
278 Programify Ltd (TNS0004)
279 Defence: Finance UIN 103360, 12 January 2026
280 HL Deb, 19 January 2026, col 18

the Government is challenging itself "to make sure current spending is fit for purpose" including ensuring the UK is ready to switch to a war-readiness footing.[281] He added that, as Chair of the Defence Oversight Board, he would look to ensure that the DIP will "chart a longer term view" which will help inform spending allocations.[282]

163. **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.

164. **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.

281 Q126
282 Q114

Annex 1: Note of Russia Policy Lab

This annex summarises the Russia 'Policy Lab' hosted by the Committee in London in January 2026.[283] This event took place in private with over 40 attendees, including experts, former diplomats and Parliamentarians. The discussion explored and challenged assumptions relating to Russia, including with reference to the Government's 2025 National Security Strategy (NSS) and other documents. Key discussion points are outlined below and informed this inquiry's recommendations.

The Russia-Ukraine war and the wider Russian threat

Some experts suggested that whatever the outcome of ongoing peace negotiations, Russia will continue to aspire to the effective erasure of Ukraine as a state, for example working to make the occupied territories' integration into Russia irreversible. The UK Government's expectation of a viable peace in Ukraine under the current peace process was criticised by some. Experts pointed to an implicit assumption that a multi-national force in Ukraine may increase European security, but warned that this is not necessarily the case.

It was argued that the cohesion of post-war society in Ukraine will relate to how the war has been fought and how it ends. It was stated that, currently, the proposed security guarantees and the 'reassurance force' are not seen as credible within Ukraine. There are fears within Ukraine that any land conceded in a peace deal could serve as a launchpad for further attacks; furthermore, it was suggested that Ukraine's defences in the Donbas have been effective in slowing Russian advances (despite Russia making claims to the entire Donbas in talks). That said, significant challenges were highlighted, including military recruitment difficulties and the need for air defences. It was suggested that an unfavourable war outcome for Russia

283 The event was designed and facilitated by the International Affairs Unit, drawing on results from Parliament's longer-term 'Russia Watch' project, which aims to strengthen understanding of futures in UK-Russia relations and is led on behalf of the Committee by the International Affairs and National Security Hub.

would not lead to state 'collapse', with some experts suggesting that a misplaced assumption about a Soviet-style collapse leads to excessive caution by Western governments.

It was suggested that Russia is no longer the great power some assume, despite permanent membership of the UN Security Council and possession of nuclear weapons. It was stated that Russia otherwise lacks 'great power' capabilities and assets, with its disinformation capabilities the primary exception. Russia's inability to defend its interests abroad beyond Ukraine was highlighted. It was stated that Russia is a junior partner of China, and that policymakers undervalue the role of China in enabling Russia. It was suggested that, despite reining in Russia on its threatened use of nuclear weapons, China has deepened its overall support for the war over time. It was recommended that the UK and its partners have candid conversations with China (with a view to bringing this support for Russia to an end) and consider further the energy dimensions of this relationship. It was suggested that growing dependency on China causes resentment in the Russian establishment, which the UK could exploit.

There was agreement that Russia poses the most significant security threat to Europe, despite challenges to the longer-term regeneration of its military capabilities. It was suggested that Russian deterrence encompasses the full spectrum of diplomatic, hybrid and nuclear activity, using tools in an agile way to achieve its aims. Experts also warned that Russia's deterrence emphasises long-range strike systems, meaning Russia may be more likely to target countries that neglect homeland defence, missile defence systems and civil defence.

Assessing UK strategy documents

The Strategic Defence Review (SDR) pointed to Russia's degraded land capabilities, but it was suggested that there is a greater need to consider the potential for Russia to attack and cause harm at a distance, for example, using air and naval assets. Some experts found it unclear from the NSS how the UK intends to increase its deterrence (beyond resilience), calling for an offensive element to deterrence that imposes meaningful costs to Moscow and takes in diplomatic, economic and military options.

There were calls for clarity on the planned spending profile for increasing UK defence spending before 2035, with increases focused on the core outputs needed to deter Russia, rather than arbitrary targets.

Some experts warned that Europe can no longer afford to consider the US as a necessary partner in NATO defence against Russia, arguing that President Trump sees Ukraine and Europe more broadly as a security burden and a low priority. President Trump, it was argued, also sees European countries

as a challenge to the US, in terms of their values and economies (although which countries was unclear). This US re-orientation away from Europe, it was argued, is likely to outlast the current US administration, reflecting a longer-term shift towards the Indo-Pacific.

The signal to the UK public and a 'national conversation'

Experts warned that, despite the UK Government's acknowledgement of the gap in defence capabilities in recent strategy documents–especially the SDR–there has been a lack of publicly discernible action to increase the pace of defence investment or to prepare for a wartime scenario. For example, little progress appears to have been made with the Defence Investment Plan, the Home Defence Programme or the promised "national conversation" on defence. It was suggested that the Government needs to do more to guide the public on how to prepare for a crisis and to communicate how it is deterring Russia, the implication being that recent strategy documents do not constitute a national conversation (despite contributing to it).

Strengthening military posture and capabilities in Europe

There was criticism of what some experts saw as a more incremental management of Russia-linked risks by the UK and its allies, with a judgement that this shut down Ukraine's ability for breakthrough and created the path to attritional war. It was recommended that European military readiness should prioritise forward defence in the Baltics and High North, as this is most likely to change Russia's risk calculus.

Some experts called for greater integration across UK and mainland Europe of the defence-industrial base, defence procurement and key capabilities for resilience in war (such as rail and road transportation systems). It was recommended that the strengthened defence-industrial base should be flexible and scalable, designed to offset US strategic reliance. It was also suggested that political will would be needed–for example, to overcome challenges linked to UK participation in the PESCO/SAFE programmes.[284] It was suggested that a new European mechanism for defence-industrial collaboration may be needed: a coalition of the willing in NATO focused

284 Permanent Structured Cooperation (PESCO) allows EU states to cooperate on military capabilities, with third parties joining projects; the Security Action for Europe (SAFE) fund supports companies in improving defence capabilities.

on funding, research and development (R&D) for strategic capabilities that may no longer be provided by the US. Generally, there was consensus on the need to integrate Ukraine into Europe's defence-industrial base, given Ukraine's unique experiences and capabilities gained in war. It was suggested that cooperation would help to sustain Ukraine economically and could mimic the Danish model of investing directly in Ukrainian manufacturing. Any risks created through closer integration would need to be managed appropriately.

It was suggested that Russia's state policy on nuclear deterrence changed significantly in 2024, when the threshold for nuclear-weapons use was lowered. There were calls for the UK to consider sub-strategic systems more fully. UK steps to join NATO's dual-capable aircraft (DCA) capability and cooperate with France on nuclear deterrence were welcomed (for example the Northwood Declaration/Nuclear Steering Group). However, it was repeatedly emphasised that there is no substitute for credible conventional deterrence, alongside the nuclear deterrent.

Changing security dynamics in the Arctic and need for greater UK attention

It was stated that Russia has significant interests in the Arctic, despite frailties that Operation Spiderweb exposed in the Russian 'Bastion'. Despite its important status in polar science, the UK was seen by some experts as not sufficiently serious in considering its Arctic interests and assets when regional stability is under challenge. There were calls for greater UK focus on Norway, as well as awareness of future challenges to both Iceland and Greenland. Svalbard and the Greenland-Iceland-UK (GIUK) gap were flagged as possible flashpoints in future.

The challenge of Russia's long-term orientation

Experts stated that Putinism is centralised, anti-western and unpredictable. It was noted that the regime is trying to ensure that Putinism outlives Putin, including among younger generations. It was recommended that Europe should be cautious about embracing a "new Russia" post-Putin when the institutional mindset may persist. It was suggested that the BBC remains one of the most trusted news sources in Russia and it was recommended that the UK expand Russian-language content, despite funding obstacles.

Conclusions and recommendations

National Security Strategy development process

1. 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. (Conclusion, Paragraph 21)

2. 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. (Recommendation, Paragraph 22)

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

4. 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. (Conclusion, Paragraph 32)

5. 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. (Recommendation, Paragraph 33)

Oversight and implementation

6. 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. (Conclusion, Paragraph 40)

7. 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. (Recommendation, Paragraph 41)

8. 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. (Recommendation, Paragraph 42)

9. 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. (Conclusion, Paragraph 46)

10. 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. (Recommendation, Paragraph 47)

Pillar 1 – Security at Home

11. 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. (Conclusion, Paragraph 57)

12. 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. (Recommendation, Paragraph 58)

13. 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. (Recommendation, Paragraph 59)

14. 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. (Conclusion, Paragraph 66)

15. 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. (Recommendation, Paragraph 67)

16. 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. (Recommendation, Paragraph 68)

17. 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. (Conclusion, Paragraph 74)

18. 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. (Recommendation, Paragraph 75)

Pillar 2 – Strength Abroad

19. 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. (Conclusion, Paragraph 79)

20. 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. (Recommendation, Paragraph 80)

21. 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. (Conclusion, Paragraph 88)

22. 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. (Recommendation, Paragraph 89)

23. 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. (Conclusion, Paragraph 104)

24. 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. (Recommendation, Paragraph 105)

25. 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). (Conclusion, Paragraph 118)

26. 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. (Recommendation, Paragraph 119)

27. 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. (Recommendation, Paragraph 120)

28. 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. (Conclusion, Paragraph 125)

29. 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. (Recommendation, Paragraph 126)

30. 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. (Conclusion, Paragraph 135)

31. 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. (Recommendation, Paragraph 136)

Pillar 3 – Sovereign Capabilities

32. 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. (Conclusion, Paragraph 151)

33. 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 utilised. (Conclusion, Paragraph 152)

34. 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. (Recommendation, Paragraph 153)

35. 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. (Recommendation, Paragraph 154)

36. 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. (Conclusion, Paragraph 163)

37. 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. (Recommendation, Paragraph 164)

Formal minutes

Monday 23 March

Members present

Matt Western (Chair)

Lord Arbuthnot of Edrom

Lord Boateng

Liam Byrne

Tanmanjeet Singh Dhesi

Lord Hutton of Furness

Lord Godson

Lord Jack of Courance

Mike Martin

Lord Sedwill

Lord Tunnicliffe

Baroness Tyler of Enfield

Sir Gavin Williamson

The National Security Strategy

Draft Report (*The National Security Strategy*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 164 read and agreed to.

Summary read and agreed to.

Annex agreed to.

Resolved, That the Report be the Fourth Report of the Committee.

Ordered, That the Chair make the Report to the House of Commons and that the Report be made to the House of Lords.

Ordered, That embargoed copies of the Report be made available.

Adjournment

Adjourned till Monday 20 April at 4.00 p.m.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 23 June 2025

Lord Peter Ricketts GCMG GCVO, Chair, Lords European Affairs Committee, former UK National Security Adviser and diplomat, Cabinet Office; **Rachel Ellehuus**, Director-General, RUSI, and former United States Secretary of Defence Representative in Europe Q1–12

Grace Cassy, Co-Founder, CyLon Ventures, External reviewer, Strategic Defence Review (2024–25), and Board Member, Ten Eleven Ventures; **Professor Michael Clarke**, Defence and Security Analyst, Sky News, Visiting Professor, King's College London, and Distinguished Fellow, RUSI Q13–20

Monday 14 July 2025

Rt Hon Pat McFadden MP, Chancellor of the Duchy of Lancaster, Cabinet Office; **Matthew Collins**, Deputy National Security Adviser, Cabinet Office Q21–35

Monday 13 October 2025

Lord Toby Harris, Chair, National Preparedness Commission; **Captain (Navy) Juha Ravanti**, Finnish Defence Attaché for UK and Ireland, Embassy of Finland; **Brigadier General Eero Rebo**, Defence Attaché, Embassy of Estonia Q36–46

Lisa Hollins, Co-Chair, Voluntary & Community Sector Emergencies Partnership (VCSEP); **Steve Vincent**, Strategic Manager, West Midlands Local Resilience Forum Q47–52

Monday 20 October 2025

Rose Gottemoeller, former Deputy Secretary General, NATO, and former Under Secretary of State for Arms Control and International Security, US State Department; **Dr Marion Messmer**, Senior Research Fellow, International Security Programme, Chatham House, and former Co-Director, BASIC Q53–64

Asoke Mukerji, former Permanent Representative of India to the United Nations, and former Deputy High Commissioner of India to the UK; **Will Todman**, Chief of Staff, Geopolitics and Foreign Policy Department, and Senior Fellow, Middle East Program, Center for International and Strategic Affairs Q65–72

Monday 3 November 2025

Isabel Hilton OBE; **The Rt Hon. the Lord Patten of Barnes KG CH**, former Governor, Hong Kong; **Nigel Inkster CMG**, former Assistant Chief and Director of Operations and Intelligence, MI6 Q73–82

Jonathan Hall KC, Independent Reviewer of Terrorism Legislation and Independent Reviewer of State Threats Legislation; **Lord Sumption OBE PC, FSA, FRHistS**, former Justice, Supreme Court of the United Kingdom Q83–93

Monday 17 November 2025

Professor Sir Anthony Finkelstein CBE, former Chief Scientific Adviser for National Security Deputy (2015–2021), and President, City St George's, University of London; **Professor Sir Nigel Shadbolt**, Executive Chair & Co-founder, Open Data Institute, and Principal of Jesus College and Professorial Research Fellow in Computer Science, University of Oxford Q94–103

Sophia Gaston, Visiting Fellow in the Department of War Studies, King's College London, and Founder and Lead, AUKUS Industry Forum; **Air Commodore (retd) Blythe Crawford CBE**, former Commandant of the Air and Space Warfare Centre, and Director GRAIL (Generative Real-Time Artificial Intelligence Lethality), Tiberius Aerospace; **Lieutenant Colonel (retd) Haydn Gaukroger OBE**, Head of Capability Development, Syos Aerospace Q104–111

Monday 26 January 2026

Rt Hon Darren Jones MP, Chief Secretary to the Prime Minister, Chancellor of the Duchy of Lancaster, and Minister for Intergovernmental Relations, Cabinet Office; **Matthew Collins**, Deputy National Security Adviser, Cabinet Office; **Dan Jarvis MP**, Minister for Security, Home Office Q112–132

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

TNS numbers are generated by the evidence processing system and so may not be complete.

1	ADS Group	TNS0007
2	British Red Cross	TNS0022
3	Roke	TNS0026
4	Council on Geostrategy	TNS0025
5	Crawford, Air Commodore Blythe	TNS0029
6	Cunning Running Software Ltd	TNS0028
7	Emergent	TNS0008
8	Gaukroger, Haydn	TNS0030
9	Gender Action for Peace and Security	TNS0021
10	Gibson, Sir Vernon	TNS0024
11	Law, Tim	TNS0005
12	McDonald, Broderick	TNS0011
13	McFarland, Mr David	TNS0003
14	MyCena limited	TNS0006
15	NCC Group	TNS0012
16	National Energy System Operator	TNS0031
17	National Preparedness Commission	TNS0001
18	Northrop Grumman UK	TNS0018
19	Programify Ltd	TNS0004
20	Rethinking Security	TNS0015
21	Saferworld	TNS0017
22	Schwarz, Professor Elke (Queen Mary University London)	TNS0010
23	Social Market Foundation	TNS0016
24	Thales UK Limited	TNS0027

25	The Centre for Finance and Security at the Royal United Services Institute	TNS0014
26	The Centre for Long-Term Resilience	TNS0009
27	The HALO Trust	TNS0019
28	Todman, Will	TNS0023
29	Waddington, Dr	TNS0013
30	iProov	TNS0002
31	techUK	TNS0020

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2024–26

Number	Title	Reference
3rd	Political finance and foreign influence	HC 720
2nd	Espionage cases and the Official Secrets Acts	HC 1414
1st	Subsea telecommunications cables: resilience and crisis preparedness	HC 723
2nd Special	Espionage cases and the Official Secrets Acts: Government and Crown Prosecution Service Responses	HC 1700
1st Special	Subsea telecommunications cables: resilience and crisis preparedness: Government Response	HC 1574