House of Commons

Business and Trade Committee

Toward a new doctrine for economic security

Eleventh Report of Session 2024–26 HC 835

Business and Trade Committee

The Business and Trade Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Department for Business and Trade and its associated public bodies.

Current membership

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

Dan Aldridge (Labour; Weston-super-Mare)

Antonia Bance (Labour; Tipton and Wednesbury)

John Cooper (Conservative; Dumfries and Galloway)

Sarah Edwards (Labour; Tamworth)

Alison Griffiths (Conservative; Bognor Regis and Littlehampton)

Sonia Kumar (Labour; Dudley)

Justin Madders (Labour; Ellesmere Port and Bromborough)

Charlie Maynard (Liberal Democrat; Witney)

Mr Joshua Reynolds (Liberal Democrat; Maidenhead)

Matt Western (Labour; Warwick and Leamington)

The following Members were also members of the Committee during the inquiry:

Gregor Poynton (Labour; Livingston); Rosie Wrighting (Labour; Kettering)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

This Report, together with formal minutes relating to the Report, was Ordered by the House of Commons, on 11 November 2025, to be printed. It was published on 24 November 2025 by authority of the House of Commons.

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

Contacts

All correspondence should be addressed to the Clerk of the Business and Trade Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 8586; the Committee's email address is commonsbtc@parliament.uk. You can follow the Committee on X (formerly Twitter) using @CommonsBTC.

Contents

Summary

The Prime Minister has been clear that economic security is national security. But the threats now facing the United Kingdom's economic security are considerable, diffuse, and growing. The global economy has become a new frontline - where supply chains, technologies, capital flows and chokepoints are increasingly used as instruments of strategic competition. The UK's adversaries are learning to weaponise interdependence while its allies are racing to build resilience. Britain must do the same.

These threats are not static. They are multiplying - and, in the years ahead, will grow exponentially. As the 'attack surface' of modern business grows and AI advances, as hostile state actors become emboldened and ownership patterns shift, the UK will witness a huge increase in the private ownership of public risk. For an open market economy like the UK's, this means that the shocks of the future - whether cyber-attacks, coercive investments, or supply-chain breakdowns - will impact the nation through the private sector first.

Economic security by its very nature can never be managed by government alone. It must become, as the Prime Minister has said of defence, a collective national endeavour through which the state, business, and society unite in pursuit of the security of the nation and the prosperity of its people.

That is why the Committee concludes that today's economic security regime is no longer fit for the future. The logic of a "whole-of-society" approach must now extend beyond defence - and become the organising principle of Britain's economic security.

Managing new risks will require remaking the way government and the market work together. Just as the national security community developed CONTEST after 9/11 to guide the fight against terrorism, so too must the UK now establish a new Economic Security Doctrine to guide the national effort in defending prosperity.

A whole-of-society approach will only succeed if it rests on long-term clarity and confidence. Government must therefore adopt a doctrine with clear strategic principles - what this Committee defines as the Six Ds:

- Diagnose emerging risks early, using shared intelligence across sectors;

- Develop domestic capability in key industries;
- Diversify critical supply chains, energy sources and technology inputs;
- Defend against hostile state and non-state actors in markets and cyberspace;
- Deter coercion and malign influence through credible counter-measures; and
- Dovetail the UK's efforts with allies to build collective strength and resilience.

To embed this doctrine, we recommend four first steps:

- The adoption of a new economic security doctrine with clear strategic principles;
- A holistic approach to threat assessment, fully involving the private sector;
- A coherent institutional framework across Government; and
- A truly whole-of-society approach, underpinned by strong public-private partnership.

To ensure the long term durability of these defences, we propose an Economic Security Bill to enshrine the approach set out in this Report in law; the appointment of a dedicated Economic Security Minister; the creation of an Office for Economic Security to coordinate policy and intelligence much as the UK established in the 1920's; the re-establishment of the Economic Security Sub-Committee of the National Security Council; reinstatement of the Secretary of State for Business and Trade as a full NSC member; and an overhaul of information-sharing with Parliament to ensure accountability.

This report marks the beginning - not the end - of that national conversation. Britain's economic security must once again become the cornerstone of its national security. In an age of economic warfare, the UK's prosperity is not merely a measure of success. It is the ultimate test of the UK's resilience and the truest expression of its strength.

Introduction

1. On 21 January 2025, the Business and Trade Committee established a Sub-Committee on Economic Security, Arms and Export Controls. The Sub-Committee was tasked with taking forward the Committee's scrutiny responsibilities in a number of areas, including arms exports licensed under the Export Control Act 2002, investment screening decisions taken under the National Security and Investment Act 2021 and thematic scrutiny of the UK's approach to economic security.

2. On 6 March 2025, the Sub-Committee launched its first inquiry to undertake a baseline assessment of UK economic security. We invited submissions responding to questions under four headings:

    a. Economic security:

        i. How should the UK Government define "economic security", and what are the advantages and disadvantages of particular definitions?

        ii. Does the UK need a clear strategy for economic security, and what are the risks of not having one?

        iii. What are the main economic security threats, and what principles should underly the UK's response to them?

        iv. Specifically, what are the challenges of new technologies, such as AI, for economic security, and how can the UK's economic security be resilient in the face of technological change?

        v. What can the UK learn from other international actors such as our allies in the United States, Europe and Japan, about how to develop an effective approach to economic security?

        vi. How can economic security be best integrated with the Government's growth mission, industrial strategy and trade strategy. What trade-offs are required between security and efficiency?

    b. Opportunities to enhance economic security:

        i. What are the most important gaps in the UK's economic security regime? How should these be addressed? What is the right level of tolerance for risk?

ii. What are the implications of managing these risks for public spending? Is HMG resourcing the management of these risks appropriately?

iii. How should the Government work with business to safeguard the UK's economic security? What is the cost to business of this approach?

iv. How should the effectiveness and success of the UK's economic security regime be measured?

c. Working across Government:

i. How should work across multiple Government departments and public bodies be co-ordinated to achieve economic security objectives?

ii. What governance structures could be put in place to ensure that economic security informs Government decision-making?

iii. What capabilities will the UK Government need to develop in order to be able to respond rapidly and effectively to economic security threats?

iv. What governance mechanisms and powers might be necessary to ensure that UK industry can respond effectively to national security threats - for example through defence production?

d. International partnerships:

i. How should the UK ensure that economic security factors into decisions around international partnerships, including trade agreements and security co-operation?

ii. How can the UK most effectively work with international partners to deter and respond to economic security threats, including economic coercion?

3. The Inquiry took in a wide variety of evidence in five ways:

a. We received over 30 written submissions to our inquiry.

b. We held a total of four oral evidence sessions between May and July 2025, exploring issues of risk analysis, investment security, critical minerals, critical infrastructure, emerging technology, cyber security and the workings of Whitehall.

c. We studied economic security policy during visits to Japan in March/April 2025, and the United States in June 2025 to learn lessons from partners

d. In March 2025, we brought together experts from business and civil society in an economic security conference held in Parliament, held under the Chatham House rule to enable a frank exchange of views and help inform the Sub-Committee's priorities.

e. Finally, in recognition of the cross-cutting nature of economic security, our inquiry has also drawn on evidence submitted to other recent parliamentary inquiries, notably the inquiry into the UK's economic security conducted by the Joint Committee on the National Security Strategy in the 2019–24 Parliament.

4. This Report sets out our baseline assessment of the UK's economic security and the policy response we now believe is required of Government. Chapter 1 outlines the approach we believe the UK Government should take to understanding economic security, through the adoption of strategic principles. In Chapter 2, we set out what we believe to be the core threats to the UK's economic security. In Chapter 3, we compare the UK's economic security "toolkit" to our key international partners. Chapters 4 to 9 set out the improvements that we believe are now required to the UK's toolkit, in order to achieve a truly "whole-of-society" approach to improving economic security in the UK.

1 Defining economic security

5. For the UK to have an effective approach to its economic security, there must first be clarity about what 'economic security' means in practice. Despite rising global threats to economic security there is no internationally accepted definition, and the UK Government has never published a definition of its own. In this chapter we consider the Government's use of the term, definitions put forward by experts and the virtue of a principles-based approach.

6. Since the 2024 general election, the Government has tied the concept of 'economic security' to various different, overlapping policy areas:

   a. National security and defence: in his introduction to the National Security Strategy, the Prime Minister said that "economic security is national security", linking it to the growth mission, and plans to reform defence procurement.[1]

   b. Trade policy: in the Trade Strategy 'economic security' is linked to the growth mission, while also connecting trade policy to supply chain resilience and the UK's ability to protect key industries through investment screening, and trade remedies.[2]

   c. Resilience: the Resilience Action Plan sets outs various initiatives for increasing broader private sector resilience, including strengthening supply chains and improving responses to other disruptive events.[3]

   d. Deterrence: the 2025 National Security Strategy recognises that "effective deterrence in the future will require more incorporation of economic measures", such as sanctions or export controls, "into our defence and security toolkit".[4]

1 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025
2 Department for Business and Trade, The UK's Trade Strategy, 26 June 2025
3 Cabinet Office, UK Government Resilience Action Plan, 8 July 2025
4 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

e. The supply of critical raw materials: the term has been used – most prominently during the passage of the Steel Industry (Special Measures) Act 2025 – to describe the importance of producing key inputs for critical sectors domestically, such as steel for the defence industry.[5]

f. Sovereign capabilities: the National Security Strategy describes the development of "sovereign capabilities", although the term is not clearly defined, as another relevant policy area.[6]

g. Industrial policy: Pat McFadden, when Chancellor of the Duchy of Lancaster with responsibility for oversight of national security policy coordination, described in his oral evidence the 'IS-8', the eight growth driving sectors set out in the Industrial Strategy, as the "starting point" for understanding the capabilities the Government wants to curate.[7]

7. When we asked the then Chancellor of the Duchy of Lancaster, whether there was either a definition or a set of principles that guides the Government's approach, he told us that the Government takes a "case-specific" approach to implementing economic security, balancing economic interests, security requirements, and policy outcomes in response to a particular circumstance.[8] Some experts supported this 'case-specific' approach. Dr Ashley Lenihan, Professor in the Practice of International Affairs at Georgetown University, told us that this gives the Government the "legal flexibility…crucial to the latitude of state action required for adaptation and survival."[9]

8. However, the Royal United Services Institute (RUSI) argued that the absence of a definition leads to "fragmented policymaking."[10] Professor Jonathan Boff, a military historian at the University of Birmingham, argued the Government's approach sees policies "dotted around in different departmental silos".[11]

---

5 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025. See also Ministry of Defence, Defence Industrial Strategy 2025: Making Defence an Engine for Growth, 8 September 2025

6 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

7 Q267

8 Q272

9 Dr Ashley Lenihan (Professor of the Practice of International Affairs at Georgetown University) (ECO0025)

10 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0012)

11 Professor Jonathan Boff (Professor of Military History at University of Birmingham) (ECO0008)

9. In particular, stakeholders drew attention to the difficulty that a lack of clear understanding within government of what economic security means presents to industry. In the words of Chatham House, an international affairs think tank, "some form of published information on the government's approach" would provide an "important signal" as to where the Government's judgment lies and what it expects from industry in response.[12] This is particularly important when managing the potential trade-offs between the Government's various economic security-related policy goals, such as growth and resilience. Lord Sedwill, former National Security Advisor, argued that if "you optimise for resilience, you cannot optimise for cost", and that therefore this tension must be resolved through the setting of a clear "common approach" across government.[13]

10. We received various suggestions for defining 'economic security' in written evidence. A selection are presented in Table 1. These definitions aspire to be broad enough to capture the range of threats to the UK's economic security, while creating a clear sense of the Government's overall objectives.

Table 1: Proposed definitions

Stakeholder	Proposed definition
Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0012)	Economic security is the ability of the UK to protect the integrity and competitiveness of its economic interests, critical infrastructure and resources, strategic industries and technologies, and research innovations against foreign threats and global shocks.
Professor Basil Germond (Chair in International Security at Lancaster University) (ECO0026)	A guaranteed and enduring access to the resources, goods, data, and underlying supply chains needed to sustain and improve the UK's economic prosperity, national security as well as the functioning of the state and the British way of life. This requires sovereign capabilities, a secure and stable global supply chain, and reliable digital communication infrastructures.

12 Chatham House (ECO0018)
13 Q50

Stakeholder	Proposed definition
Dr Nicola Searle (EC00006)	Economic security is the stability and resilience of the UK economy and UK economic growth. It includes the stability of employment, the protection of standards of living, the resilience of the economy to inflation and shocks and the support of economic growth through UK innovativeness. It is a whole-society approach, rather than a business-centric definition. Economic security is a long-term and dynamic concept.

Principles or a formal definition?

11. When we put the possible adoption of a formal, singular definition to the then Chancellor of the Duchy of Lancaster, he argued that rather than improving clarity it would generate more confusion for businesses. He told us that the adoption of a definition could lead to legal complexities as firms might allege that the Government was acting in a way that was incompatible with its own terms.[14] Sir Simon Fraser, Founding Partner at Flint Global, a business advisory firm, concurred. He said that in a "fast-moving environment", Government may spend "an awful lot of time trying to reach agreement on a definition and then find that it has changed". Alexandra Kellert, Associate Director at Control Risks, a London based global risk consultancy, told us that potentially having to "constantly revise those definitions" could create instability and therefore lead to a decrease in business confidence.[15]

12. There is, however, an approach other than a formal definition which can supply clarity, predictability and consistency. A principles-based approach has most commonly been adopted in other jurisdictions that we studied, such as the European Union and Japan. In their written evidence to the Joint Committee on the National Security Strategy (JCNSS), the previous Government also adopted a principles-based framework.[16]

14 Q271
15 Q12
16 Joint Committee on the National Security Strategy, The UK's economic security, Cabinet Office (UKE0013)

Table 2: Comparison of economic security principles

Country	Objectives
Japan	Self-sufficiency: reducing supply chain dependence on certain countries, such as China. Advantage and indispensability: increasing its trade partners' dependence on Japan via focussing on superiority in emerging technology. Safeguarding the rules-based international system.[17]
European Union	Promoting competitiveness. Protecting from economic security risks. Partnering with allies to cooperate on economic security.[18]

13. The then Chancellor of the Duchy of Lancaster said that the Government uses a 'promote, protect, and partner' framework. These are the same principles used by the European Union. It was unclear whether these terms had been formally adopted by the UK Government, or if they simply act as a more informal internal guide to desired policy outcomes.[19] The absence of an explicit acknowledgement of this framework in policy documents, such as the National Security Strategy or the Trade Strategy, suggests the latter.

14. The Centre for Inclusive Trade Policy and the UK Trade Policy Observatory told us that a principles-based approach enables governments to be more responsive to the risks generated by a "rapidly evolving global economy".[20] They argued that, unlike a fixed definition, flexibility means that the approach can be adapted to any "new economic, technological, or geopolitical risks" that may emerge.[21] RAND Europe, a research organisation, also said that the adoption of "key objectives" provides more "clarity for government and businesses" as they establish a shared understanding of what the Government's goals are when it seeks to deliver 'economic security' related initiatives.[22]

17 Japanese Ministry of Economy, Trade and Industry, Japan's National Security Strategy (PDF), 2023, section 2

18 European Commission, Strategic Autonomy and European Economic and Research Security (accessed 7 November 2025)

19 Q272

20 Centre for Inclusive Trade Policy and UK Trade Policy Observatory (ECO0014)

21 See previous reference

22 RAND Europe (ECO0021)

Table 3: Proposed principles

Stakeholder	Principles
Oxford China Policy Lab (EC00016)	Ensuring continuous stability. Protecting against foreign powers' exercise of "weaponized interdependence". Safeguarding world class research and innovations.
RAND Europe (EC00021)	Safeguarding and advancing economic prosperity and growth. Securing access to and protection of defence capabilities. Retaining ability to conduct economic warfare.

15. Critics of this approach may suggest that it still creates too much ambiguity for policymakers and businesses. For example, members of RUSI's European Economic Security Taskforce argued that when considering the European Union's 'three pillars' there is a lack of clarity in understanding "how much weight to place on each of the three pillars".[23] It was suggested that the 'promote' and 'protect' pillars "often conflict in the context of supply chains", and that the absence of clearly defined goals means "it is almost impossible to differentiate between supply chain risks [and] prioritise sectors according to their vulnerabilities". Nevertheless, contributors put forward various methods for improving shared understanding and aligning action. The creation of decision trees, for instance, was highlighted as a useful tool for understanding which pillar should first be prioritised.[24]

16. The UK Government has recognised the value of a principles-based approach to shape its response to threats faced in the past. CONTEST, for example - the UK's counter-terrorism strategy - was first developed to coordinate the pan-Governmental response to the new terrorist threats that multiplied after the 9/11 terrorist attacks. CONTEST is divided into four pillars or workstreams: Prevent, Pursue, Protect, and Prepare.[25] It has stood

23 RUSI, RUSI European Economic Security Taskforce Meeting 1: The Conceptual and the Concrete, 18 October 2024, p8

24 A decision tree is a diagram that shows the different choices and possible outcomes of a decision. See previous reference

25 Prevent: to stop people becoming terrorists or support terrorism; Pursue: to stop terrorist attacks; Protect: to strengthen protection against a terrorist attack; Prepare: to mitigate the impact of a terrorist attack.

the test of time; successive governments have maintained this framework, describing its value in creating a shared sense of purpose, while remaining adaptable as threats evolve.[26]

A "whole of society" approach

17. In his foreword to the Strategic Defence Review in June 2025, the Prime Minister highlighted the need for a "whole-of-society" approach to defence, described as "a collective national endeavour through which the state, business, and society unite in pursuit of the security of the nation and the prosperity of its people".[27] We have heard throughout our inquiry that the need for a whole-of-society approach goes beyond defence, and is just as essential for economic security. We have also seen examples of this approach working in other jurisdictions; during our visit to Japan, we heard how Keidanren (the Japan Business Federation) had been part of an expert panel convened to help design Japan's Economic Security Protection Act.

18. However, it is clear that before the state can pull together business and society in the collective effort of economic security, it must first ensure a coherent whole-of-government approach. This was put to us clearly by Dr Francesca Ghiretti, Director of the RAND Europe China Initiative, who concluded that "we first need a cross-Government economic security approach and then we can talk about a whole-of-society approach".[28]

19. **CONCLUSION**
Economic security is fundamental to national security. We welcome the Government's recognition of this. By its very nature however, only industry and Government working jointly and severally together can safeguard the UK's economic security through the 'whole of society approach' to defence which the Prime Minister has said the times now require. New safeguards however will not come without cost. On the contrary, a stronger defence of our economic security will require sustained long-term public and private investment. This in turn will require both clarity and certainty about the Government's objectives, well beyond the life of one Parliament.

26 Home Office, Counter-terrorism strategy (CONTEST) 2011, July 2011; Home Office, Counter-terrorism strategy (CONTEST) 2018, June 2018; Home Office, Counter-terrorism strategy (CONTEST) 2023, July 2023

27 Ministry of Defence, The Strategic Defence Review 2025 - Making Britain Safer: secure at home, strong abroad, 2 June 2025, p2

28 Q45

20. **CONCLUSION**

In the face of a fast-changing international environment, a fixed, formal definition of 'economic security' is likely to be unworkable. However, as demonstrated by CONTEST, Government can guide policymakers and businesses by clearly setting out the principles of a long-term approach in a new and clearly articulated economic security doctrine.

21. **RECOMMENDATION**

The Government should adopt, and clearly set out, the strategic principles of a new doctrine for economic security. From our consideration of the evidence and comparisons with other jurisdictions, we recommend that this might best incorporate six core principles - the '6Ds':

- Diagnose and regularly share an understanding of threats to the UK's economic security.
- Develop sovereign capabilities in areas critical for UK economic security.
- Diversify critical supply chains, energy sources and technology inputs to reduce risks of disruption and coercion, through combined action with allies.
- Defend critical and vitally significant infrastructure, other important national assets such as data, intellectual property to prevent technology leakage, and critical sectors through building resilience, especially in cyber space.
- Deter threats to UK economic interests through proactive enforcement of offensive economic measures, such as sanctions, at home and abroad.
- Dovetail public-private co-operation domestically and internationally, aligning and collaborating with allies, and ensuring a concerted and joined-up effort across the nation and the UK's alliances.

22. **CONCLUSION**

Safeguarding economic security will always involve calculated trade-offs. Principles will often conflict. No government therefore can eliminate all ambiguity for businesses and policymakers. This is where political leadership is crucial. It is for the Government to set out how it has chosen to make trade-offs and to prioritise between different principles in any given situation. In turn, it is for Parliament to scrutinise the choices made by Government, to challenge and ensure democratic legitimacy.

23. **RECOMMENDATION**
To ensure both clarity and long-term certainty for the UK's economic security regime, the Government should consider enshrining the key recommendations in this Report via a new Economic Security Bill. This would allow Parliament to be fully engaged in providing a new, stronger foundation to the UK's economic security.

24. This Report sets out the steps we believe are necessary to achieve this whole-of-society approach. Chapter 2 outlines the threat landscape facing the UK, and Chapter 3 considers the reforms to the machinery of government needed to meet this challenge. Chapters 4 to 9 then look at individual aspects of the UK's economic security "toolkit", setting out how government and industry can work together more effectively to pursue the six strategic economic security principles we have enunciated.

2 Threat assessment

25. An effective approach to economic security must begin with a diagnosis of the current threats to the UK's economy. Contributors to our inquiry described an international environment characterised by growing turbulence and volatility.

26. Antony Walker, Deputy CEO of techUK, a trade association for the UK technology sector, told us that UK industry was now operating in a "far more complex and interdependent, but also more fragmented world".[29] We were told that the growing complexity of the global economy and its changing profile, as well as its digital interconnectedness, mean that new risks have emerged. The new risks in the world require more businesses than ever before to consider the impact of political and geopolitical risk on their operations.[30]

27. The UK Government recognises the environment in which it operates but has not published a single consolidated assessment of the threats to UK economic security. Instead, aspects of economic security feature in at least five separate Government assessments of threat and risk (see Table 4).

Table 4: UK Government risk and threat assessments

Document	Summary	Threat assessment
The National Security Strategy (NSS), June 2025	The NSS aims to "identify the main challenges we face as a nation in an era of radical uncertainty", and then to "set out a new Strategic Framework in response, covering all aspects of national security and international policy".	The NSS sets out a "strategic context" characterised by "radical uncertainty".[31]

29 Q131
30 Q8; Q265; Q22
31 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

Document	Summary	Threat assessment
The Strategic Defence Review (SDR), June 2025	The Strategic Defence Review was led by three external Reviewers. It considered the threats the UK faces, the capabilities it needs to meet them, the state of UK armed forces and the resources available.	The SDR describes the UK entering "a new era of threat and challenge", with a world "more volatile and more uncertain than at any time in the past 30 years and [...] changing at a remarkable pace".[32]
The National Risk Register, January 2025	The National Risk Register is the external version of the National Security Risk Assessment (NSRA), which is the Government's assessment of the most serious risks facing the UK.	The most recent NRR includes information about 89 risks, within 9 "risk themes".[33]
The UK Government Resilience Action Plan, July 2025	The Resilience Action Plan has three objectives: to continuously assess how resilient the UK is to target interventions and resources effectively; to enable the whole of society to take action to increase their resilience; and to strengthen the core public sector resilience system.	Referencing the NSS, the Resilience Action Plan describes the UK as facing "volatile, varied and interconnected" risks.[34]
The Defence Industrial Strategy, September 2025	One of the eight "priority sector plans" arising from the Government's Industrial Strategy.	It references the SDR's description of "a new era of threat", and links this to economic challenges and opportunities, noting that "security and prosperity have become inextricably linked and intertwined".[35]

32 Ministry of Defence, The Strategic Defence Review 2025 - Making Britain Safer: secure at home, strong abroad, 2 June 2025
33 Cabinet Office, National Risk Register 2025, 16 January 2025
34 Cabinet Office, UK Government Resilience Action Plan, 14 July 2025
35 Ministry of Defence, Defence Industrial Strategy 2025: Making Defence an Engine for Growth (PDF), 8 September 2025

28. Given the diffuse nature of economic security threat assessments, spread across multiple overlapping Government strategies and plans, we wrote to Lord Robertson in his capacity as SDR lead reviewer, asking for the Review Team's assessment of economic security threats, and whether the Review Team had learned anything about our economic security that was not featured in the SDR.[36] Lord Robertson asked the Ministry of Defence to provide us with this information. We are grateful to Lord Robertson for his support with our inquiry.

29. In the Ministry of Defence's response, received in August 2025, Defence Minister Lord Coaker told us that "in recent years, there has been significant growth in the use of a range of economic levers to undermine the national security of the UK and its allies", necessitating a "whole-of-government response" to counter. Lord Coaker described the recent National Security Strategy as "the key document that sets out the approach to economic security as a core part of our national security". The Minister drew attention to six "principal threats" that were included in the National Security Strategy, which all have at least some potential economic security element:

- Hostile state activity;
- Strategic competition and confrontation;
- Economic and technological vulnerabilities;
- Terrorism and extremism;
- Organised crime and illicit finance; and
- Climate, health and demographic shocks.

30. In response to our specific question about whether economic tools might be used against the UK by its adversaries, the Government stated that identifying the "intent and origin of economic actions that impact national security" can be "challenging", as they may operate from a state level down to the actions of individual companies or investors. The Minister also noted that actions with a "legitimate economic purpose" may still impact on national security interests "either deliberately or inadvertently".[37]

36 Letter from the Chair to Lord Robertson relating to the Strategic Defence Review (PDF), 10 July 2025

37 Letter from the Lord Coaker to the Chair relating to questions raised on the UK's economic security in response to the Strategic Defence Review (PDF), 27 August 2025

31. **CONCLUSION**
The Government has published a multitude of security reviews and sectoral evaluations, but not a single consolidated assessment of the threats to UK economic security. Given the lack of a "single source of truth", we have decided to summarise our own baseline assessment of economic security threats. We hope that Parliament will enhance and develop this 'parliamentary view' over the years ahead. From our evidence, we have identified ten elements of the threat landscape facing the UK economy:

- **i.** Transnational risks;
- **ii.** Disruption to worldwide market competition;
- **iii.** State threats, including the coercive use of economic tools;
- **iv.** Supply chain disruptions, along with threats to transport and sea lanes;
- **v.** Critical minerals;
- **vi.** Critical National Infrastructure (CNI);
- **vii.** Cyber and emerging technology;
- **viii.** Illicit finance and money laundering;
- **ix.** Foreign investment in critical sectors of the UK economy; and
- **x.** People-focussed threats, such as intellectual property (IP) theft or physical threats to executives.

32. **CONCLUSION**
Together these threats point to a transformed threat landscape in which we are likely to see a radical expansion in the private ownership of public risk. This underlines the absolute imperative of rethinking the way state and market work together to safeguard economic security. Most challenging of all is the reality that rarely will any single one of these risks present alone. Instead, they may combine in ways that the UK may struggle to manage.

33. The remainder of this chapter provides more detail on each of the ten threats we have identified.

(1) Transnational risks

34. The 2025 National Security Strategy argues that in the coming years the UK will have to contend with "the effects of climate change and potential ecosystem collapse, biological threats, demographic shifts, continued urbanisation, [and] threats to human health".[38] We were told that these trends are already having a profound impact on the UK economy. Trevor Hutchings, CEO of the Renewable Energy Association, said that his sector was already experiencing the "disruption" that "flooding, high winds, or storm damage" causes.[39] Academics from the Grantham Institute at Imperial College London argued that policymakers currently "underestimate the risks associated with physical climate impacts", generating significant concerns as to the future resilience of the UK's infrastructure.[40]

35. **CONCLUSION**
The UK faces increasingly complex transnational threats. The devastating impacts of the Covid-19 pandemic and the rapidly changing climate are two examples of existential challenges, against which the UK economy must become more resilient.

(2) Disruption to worldwide market competition

36. After a long period of opportunity after the creation of the World Trade Organization (WTO),[41] the global rules of competition are now in turmoil.[42] Witnesses described UK firms as battling in a world where the rules that govern global trade are breaking down. Dr Francesca Ghiretti, Director of the RAND Europe China Initiative, told us that there was no longer a level-playing field for firms internationally, with states that follow "the international rules in terms of subsidies and competition" unable to compete with those that flout them.[43] Henrik Pederson, CEO of Associated

38 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025
39 Q123
40 Jenny Bird (Campaign Manager at Grantham Institute, Imperial College); Raffaele Della Croce (Senior Research Fellow at Centre for Climate Finance & Investment, Imperial College Business School); Dr Ajay Gambhir (Director of Systemic Risk Assessment at Accelerator for Systemic Risk Assessment (ASRA); Grantham Institute, Imperial College London) (ECO0022)
41 The WTO is a multilateral organisation where countries meet to agree on trade rules, review trade policies, and settle trade disputes.
42 The Committee has explored this theme throughout its Export led growth inquiry, see for example the report on trade with the Asia-Pacific region.
43 Q41

British Ports, argued that other countries had found ways to interpret WTO rules in such a way that favoured "their companies and home-grown industries". He concluded that as a result, the UK is now "losing out".[44]

37. **CONCLUSION**
The UK faces unprecedented disruption to the international economic order. As many powers prioritise self-interest above adherence to the rules-based system, the UK economy faces new risks of economic damage that may jeopardise the UK's growth objectives.

(3) State threats, including the coercive use of economic tools

38. Pat McFadden, then Chancellor of the Duchy of Lancaster, told us that we require much greater vigilance of state threats—including overt or covert action by states intended to harm or undermine competitors, below the threshold of military force. The Minister described the shift from terrorism led by non-state actors, towards state-backed threats as the "biggest change in the threat landscape in recent years".[45]

39. The threat from the UK's state adversaries is serious. The 2025 National Security Strategy said that "hostile activity on British soil from countries like Russia and Iran is increasing, threatening our people, critical national infrastructure, and prosperity".[46] Catherine Royle, Political Advisor to the Commander at NATO, Joint Command Brunssum, told us that state adversaries are looking for "any sign of weakness in our institutions and where they think it is going to be difficult for us to respond".[47] This manifests across many of the methods of attack outlined below, such as cyber-attacks or espionage. Globalisation[48] and the development of complex global supply chains have also created ample opportunity for countries to use economic tools and interdependence as a means of pursuing their wider strategic goals.[49]

44 Q142
45 Q264
46 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025
47 Q40
48 Broadly defined as the free flow of goods, services, people, money, capital and technology.
49 ADS Group (ECO0002); Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

40. The Government primarily talks about 'state threats' in relation to Russia, China, Iran and North Korea. But China has been identified by successive government strategies since 2021 as posing a range of threats to UK economic security.[50]

41. Foreign-owned companies can now provide a vector for these threats. Hitherto, government analysis has focussed less on the asymmetric disadvantage to the UK created by what is otherwise a fundamental strength of free markets: while the duties of UK companies' are primarily owed to their shareholders, in contrast China and Russia can exercise a degree of political control over how their companies behave.[51] Economist Rebecca Harding argues this "tension between nation states and corporates" caused by misaligned goals and incentives is the "defining challenge of our era" for the West.[52]

42. New risks are also now generated from allied action not least, the uncertainty generated by President Trump's approach to foreign and domestic policy. Catherine Royle said that it was currently unclear what "US foreign and security policy is".[53] The United States is the UK's largest trading partner, accounting for 17.8% of total UK trade.[54] As a result, we heard that the America First Trade Policy - most obviously manifested in the administration's imposition of wide-ranging tariffs on goods imported into the US - has had a significant impact on the critical sectors of the UK economy. Our report on the US Economic Prosperity Deal found that many of these industries, such as steel and pharmaceuticals, remained in "a state of uncertainty about the future tariffs regime they may face."[55]

---

50 HM Government, Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy, March 2021; HM Government, Integrated Review Refresh: Responding to a More Contested and Volatile World, March 2023; Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

51 Centre for Economic Security (ECO0003); Coalition on Secure Technology (ECO0015); Dr Ashley Lenihan (Professor of the Practice of International Affairs at Georgetown University) (ECO0025)

52 Rebecca Harding, The World at Economic War: How to Rebuild Security in a Weaponized Global Economy (London: London Publishing Partnership, 2025)

53 Q46

54 Department for Business and Trade, Trade and Investment Factsheets: United States (PDF), 31 October 2025

55 Business and Trade Committee, US Economic Prosperity Deal, HC 1306, 14 September 2025, para 48

43. **CONCLUSION**
Threats to the UK from state actors that fall short of military action are continuing to grow. Foreign powers are increasingly willing to coerce or undermine others using economic tools or by exploiting economic interdependencies. Russia, China, Iran and North Korea are most often cited as being directly or indirectly responsible for hostile acts targeting the UK. However, actions taken by the UK's allies—as part of intensifying political, economic and technological competition globally—also contribute to geopolitical uncertainty and economic instability.

(4) Supply chain disruptions, transport and sea lanes

44. The inter-connectivity and complexity of the global economy means that the impacts of supply chain disruptions, such as following the Covid-19 pandemic or Russia's full-scale invasion of Ukraine in 2022, have increased and become more unpredictable. This complexity often means that it is impossible for the company making the final product to trace production all the way back to the original raw materials. For instance, ADS Group told us that there around "6,000 or 7,000 smaller contractors" in the supply chain of a large defence company.[56] Following a disruption, such as the recent Covid-19 pandemic, it might then take 18–24 months to source alternative suppliers.[57] There is evidence that, in a worsening security environment, the likelihood of largescale future supply chain disruptions has increased significantly.[58]

45. As an island nation, many of our critical supply chains rely on secure shipping lanes, ports and undersea infrastructure, such as subsea cables.[59] Around 90% of the world's trade is conducted by sea,[60] international trade (exports plus imports of goods and services) was equivalent to 62% of UK GDP in 2024[61] and according to the Government's 2025 National Security Strategy, £65 billion of UK economic activity relies on the subsea cable

56 Q118
57 Q126
58 Bearman et al., Shock transmission, global supply chains, and development: assessing responses to trade shocks (PDF), Bank of England Staff Working Paper No. 1,092, August 2024
59 The UK's ability to defend its undersea infrastructure was recently examined by the Joint Committee on the National Security Strategy, in their report Subsea telecommunications cables: resilience and crisis preparedness, HC 723, 19 September 2025.
60 International Chamber of Shipping, Shipping and World Trade: World Seaborne Trade (accessed 14 October 2025)
61 WTO, Trade Policy Review: United Kingdom – Executive Summary (PDF), 30 October 2025, para 1

industry.[62] The accidental or deliberate disruption of maritime supply chains can therefore lead to significant economic impacts. For example, in July 2025, it was reported that, following attacks by the Houthis, the insurance cost of shipping goods through the Red Sea had more than doubled.[63] While the 2025 Strategic Defence Review argued that the "Royal Navy should play a new leading and coordinating role in securing undersea pipelines, cables, and maritime traffic,"[64] there are long-standing concerns as to the size of the fleet[65] and there is a challenge as Professor Basil Germond, Chair in International Security at Lancaster University put it, squaring our "overstretched resources" with these "increasing demands".[66] The complexities here are underscored by Ireland in whose waters many of the cables critical to British connectivity sit. Of all the transatlantic subsea cables in the Northern Hemisphere, some 75% pass through or close to the Irish Exclusive Economic Zone.[67] However, Dublin has no current underwater capability, and adding just one military sonar system is a big-ticket item. A contract to defence firm Thales is said to be worth 'multi-millions'.[68]

46. **CONCLUSION**

The world has never been more interconnected, and the UK economy is dependent on complex and interwoven supply chains. Consumers, businesses and public institutions rely on supply chains where objects repeatedly cross borders, often on a "just-in-time" basis where the slightest disruption can have enormous impacts. The complexity of supply chains promotes efficiency, low prices and consumer choice, but leaves the UK economy vulnerable.

47. **CONCLUSION**

Maritime infrastructure, together with the UK's telecommunications and energy systems, underpin these supply chains. The events of recent years, notably Houthi attacks on commercial ships in the Red Sea, have demonstrated the continuing centrality of maritime security to the UK economy. Increasing global instability means maritime security is more important than ever.

62 HM Government, National Security Strategy 2025: Security for the British people in a dangerous world, June 2025, p. 23

63 "Red Sea insurance soars after deadly Houthi ship attacks", Reuters, 10 July 2025

64 Ministry of Defence, The Strategic Defence Review 2025 - Making Britain Safer: secure at home, strong abroad, 2 June 2025

65 See for example, Defence Committee, "We're going to need a bigger Navy", HC168, 14 December 2021

66 Joint Committee on the National Security Strategy, The UK's economic security, Professor Basil Germond (Professor of International Security at Lancaster University), UKE0001

67 RUSI, Ireland's Defence Deficit, 21 December 2022

68 Irish Department of Defence, Tánaiste announces major new contract for Sonar Capability, updated 18 June 2025

(5) Critical minerals

48. Europe, including the UK, consumes approximately 30% of the world's critical mineral production,[69] but only produces 2–3% of global supply.[70] For many of these minerals, the UK also lacks a significant domestic presence at key points in the value chain, with its refining and manufacturing capacity at a "nascent stage", according to the UK Critical Minerals Intelligence Centre.[71] This leaves the UK vulnerable to supply chain turbulence, and the weaponisation of this dependency in particular. China dominates the majority of the UK's critical mineral supply chains. Of the 34 critical minerals identified in the Critical Minerals Intelligence Centre's 2024 UK Criticality Assessment, China is the primary producer of 21.[72] Mike King, Business & Government Relations Vice President at Cornish Lithium, told us that China has "started to weaponise some of the other rare earths and rare minerals that [it] either produces or processes".[73] Following the US' imposition of higher tariffs on Chinese goods in April 2025, China tightened its rare earth export controls, before putting in place new restrictions in October.[74] This suggests the ways in which these ten risks can reinforce one another.

49. More broadly, John Lindberg, Policy & Government Affairs Principal at the International Council on Mining and Metals, told us that there is a "trend across the world" of increasing export restrictions and bans.[75] Analysis by the OECD, published in 2024, contended that due to the increase in demand for these materials, driven by the green and digital transitions, there are growing incentives for suppliers to "exploit market power dynamics to pursue economic and non-economic objectives".[76] Academics from the University of Exeter and University College London described this geopolitical climate as one of increasing resource "nationalism,

69 Minerals, or more broadly raw materials (other than fuel), are described as 'critical' if they are essential to a state's economic or national security and have a supply chain that is particularly vulnerable to disruption.

70 Dr Kathryn Moore (Senior Lecturer in Critical and Green Technology Metals at Camborne School of Mines, University of Exeter); Dr Bridget Storrie (Teaching Fellow at The Institute for Global Prosperity, University College London) (ECO0034). See also, Foreign Affairs Committee, A rock and a hard place: building critical mineral resilience, HC 371, 15 December 2023, para 6

71 UK Critical Minerals Intelligence Centre, UK 2024 Criticality Assessment (PDF), 28 November 2024

72 See previous reference

73 Q94

74 "China tightens export rules for crucial rare earths", BBC News, 9 October 2025

75 Q107

76 OECD, OECD Inventory of Export Restrictions on Industrial Raw Materials (PDF), September 2024

protectionism and competition".[77] The competitive nature of the global marketplace was recently demonstrated by Pensana, a UK-based rare earths company, dropping its plans to build a refinery in Hull. Paul Atherley, Pensana's Chairman, was quoted as saying that the UK Government's £5 million contribution to the project was "nowhere near enough", especially compared to the support being offered to the sector by the US government.[78]

50. **CONCLUSION**
Over the coming years, emerging technologies and the net zero transition will increase global demand for critical minerals exponentially. The absence of any significant domestic presence in the mineral value chain leaves the UK significantly exposed to disruptions in their supply. There is considerable potential for adversaries to use this to their advantage, while the UK has no equivalent strategic leverage.

(6) Critical National Infrastructure (CNI)

51. The UK's critical national infrastructure (CNI), such as energy and water supply lines and core transport infrastructure, is fundamental to the functioning of society and the UK economy.[79] An uncertain international environment, and the effects of climate change, mean that the UK's CNI operators must now prepare to mitigate more risks than ever before.[80] These range from espionage, physical intrusion, power outages, cyber-attacks, supply chain disruptions, to exposure to extreme weather events.[81] The impact of CNI failure can be catastrophic. It was estimated that the economic cost of a major power outage affecting Spain, Portugal and parts of France earlier this year was between 2.25 billion and 4.5 billion euros.[82]

52. There is also the risk that overreliance on foreign suppliers to the UK's CNI creates a source of vulnerability that might be deliberately exploited or susceptible to shock. Of particular concern is the UK's renewable energy supply chain, in which China is a dominant supplier. China's 2017 National

77 Dr Kathryn Moore (Senior Lecturer in Critical and Green Technology Metals at Camborne School of Mines, University of Exeter); Dr Bridget Storrie (Teaching Fellow at The Institute for Global Prosperity, University College London) (ECO0034)

78 "Major UK rare earths refinery scrapped in favour of US", BBC News, 17 October 2025

79 The UK defines its critical national infrastructure (CNI) as "certain 'critical' elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life". This includes assets such as energy supply pipelines, transport infrastructure and water supplies. National Protective Security Authority, Critical National Infrastructure, 23 June 2025

80 Q129

81 Q123; Q126; Q131; Q144

82 According to RBC, as quoted in "Spain, Portugal, switch back on, seek answers after biggest ever blackout", Reuters, 29 April 2025

Intelligence Law obliges Chinese companies and citizens to "support, assist, and cooperate with national intelligence efforts in accordance with law".[83] As a result, Chinese companies could be compelled to support the intelligence gathering efforts of the Chinese government. Trevor Hutchings, CEO of the Renewable Energy Association, told us that it was currently unclear to his members as to what an acceptable level of Chinese involvement is in a "particular subsector, particular technology, or any particular industry".[84] The Council on Geostrategy, a foreign policy and defence think tank, contended that China's dominance of these supply chains, and the Government's ambitious clean energy targets, will generate difficult trade-offs for policymakers between "economic growth, security and climate considerations".[85]

53. **CONCLUSION**
The UK's existing critical national infrastructure is vulnerable to a range of threats, from extreme weather to cyber-attacks. In expanding and renewing that infrastructure in response to a growing population and the net zero transition, the UK may be forced to re-evaluate the trade off between on the one hand, lower cost technology and investment from China, and on the other, the risks to resilience that would entail.

(7) Cyber and emerging technology

54. As IT systems become increasingly vital to the functioning of society and the economy, so too are they increasingly valuable targets for a variety of malicious activities. Katharina Sommer, Group Head of Government Affairs and Analyst Relations at the cyber security firm NCC Group, told us that, to some extent, everything relies on "digital technology…that has just broadened the attack surface massively, so there are targets everywhere nowadays".[86] More actors are now involved in these attacks. The main perpetrators remain China, Russia, Iran and North Korea.[87] However, Richard Horne, CEO of the National Cyber Security Centre, told us that it was "almost a bit too simple to say 'nation state' and 'criminal' now".[88] Chris Parker, Director Government Strategy at Fortinet UK, a cybersecurity

83 China Law Translate, PRC National Intelligence Law (as amended in 2018), June 2017
84 Q136
85 Council on Geostrategy (ECO0019)
86 Q217
87 National Cyber Security Centre (NCSC), NCSC Annual Review 2025, 14 October 2025, pp20–21
88 Q238

company, described the "almost commercialisation" of crime, through which private enterprises create the capabilities cyber criminals or nation states purchase to undertake malicious activities.[89]

55. These attacks have also increased in sophistication, with emerging technologies such as artificial intelligence (AI) significantly reducing the time required for attackers to exploit compromised systems. James Babbage, Director General (Threats) at the National Crime Agency, told us that AI was already allowing threat actors to "automate some of the earlier stages" of cyber-crime.[90] Zeki Turedi, Field Chief Technology Officer, Europe at the cybersecurity company CrowdStrike, said that five years ago it would have taken around 10 hours on average for a threat actor to get into an organisation's system. Today, "it is less than one hour, and the best time is 51 seconds".[91]

56. **CONCLUSION**
Cyber threats to the UK's economy, institutions and infrastructure continue to evolve. A string of high-profile attacks in 2025 have vividly demonstrated the devastating impacts of these attacks on workers, consumers and associated supply chains. The boundary between "state" and "non-state" cyber-attackers is becoming increasingly blurred, and the rapid emergence of new technologies will exponentially multiply the damage they can inflict.

(8) Illicit finance and money laundering

57. Financial services is one of the largest sectors of the UK economy, contributing £208.7 billion to the economy in terms of gross value added (GVA) in 2024. This was 8% of total UK GVA.[92] However, the City of London's status as a leading global financial centre also creates vulnerabilities. There is evidence of loopholes in UK company law being used to conceal money laundering, sanctions evasion, and other types of illicit finance. In 2023, it was alleged that the Russia-linked Seychelles-based Alpha Consulting helped to form 900 UK limited partnerships (LPs), in order to conceal the true owner of UK-registered assets. Some of the beneficial owners of these LPs were described as members of Vladimir Putin's "inner circle".[93] Ben Cowdock, the Senior Investigations Lead at Transparency International, told us that there were "undoubtedly" UK registered companies being used

89 Q102
90 Q241
91 Q102
92 Office for National Statistics, GDP output approach - low level aggregates, 30 September 2025
93 "Criminals and sanctions-busters exploiting UK secrecy loophole", BBC News, 2 November 2023

to "circumvent sanctions".[94] When we asked Companies House how many companies on the register contained false information, they told us that it was likely to be around 15–20% (around 750,000–1,000,000 companies).[95]

58. **CONCLUSION**
The UK's long-standing status as a global financial centre is both a crucial economic strength, and a potential vulnerability that must not be overlooked. Inadequate safeguards against sanctions evasion and money laundering risk undermining the effectiveness of the UK's economic security toolkit.

(9) Foreign investment in critical sectors of the UK economy

59. As the UK Government seeks foreign investment to boost growth, there is a risk that dependencies are created, reducing the UK's strategic autonomy in critical sectors of the economy. The Centre for Economic Security, a research and convening organisation, raised concerns with US private equity investment into UK defence companies: "The risk is that our innovative defence capability feeds more directly once it is in the growth phase into US capability rather than ours".[96] In the context of emerging technologies, Boardwave, a scale-up accelerator for technology businesses, warned that "UK-developed intellectual property and expertise are increasingly absorbed by larger foreign firms, further weakening the UK's economic resilience and strategic autonomy".[97] This issue is about to become more acute. The Government's plans will require the mobilisation of large-scale investment into critical parts of the UK economy. Over the next ten years this additional investment may total up to £1 trillion.[98]

60. **CONCLUSION**
The UK's reliance on foreign direct investment risks a loss of control over emerging companies in industries critical to the national interest. Capabilities developed by the UK defence and emerging technology sectors are increasingly being targeted by foreign firms and governments.

94 Business and Trade Sub-Committee on Economic Security, Arms and Export Controls, Oral evidence: Economic Crime, HC 798, Q14
95 Business and Trade Sub-Committee on Economic Security, Arms and Export Controls, Oral evidence: Economic Crime, HC 798, Q32
96 Centre for Economic Security (ECO0003)
97 Boardwave (ECO0020). We will be exploring this issue further through our financing the real economy inquiry.
98 The Capital Markets Industry Taskforce, The Capital Markets of Tomorrow (PDF), 6 September 2024, p. 6

(10) People-focussed threats

61. The talent of the UK is amongst its greatest assets, but this is now being directly targeted by hostile actors. This may take the form of intellectual property theft, espionage, or physical threats towards senior executives involved in critical sectors of the UK economy. In 2024, MI5 briefed vice-chancellors from 24 universities on the threats posed by foreign states "intent on stealing intellectual property to enhance their own economic and military capabilities".[99] Later in the same year, it was reported that Russia had attempted to assassinate the CEO of a German defence company.[100] Alexandra Kellert said that Control Risks, a global risk consultancy, had seen a "significant uptick in the requests that our security-focussed teams get from companies for us to carry out threat assessments specifically on their executives. That has definitely, over the past year or so, been a huge change."[101]

62. **CONCLUSION**
In increasing the resilience of institutions and technology, the UK must not lose sight of people-based threats. People are an organisation's greatest asset, but they can also be its most unpredictable vulnerability. The UK's adversaries can be expected to target individuals for influence, blackmail, espionage and even physical harm. As more sectors of the economy are recognised for their importance to economic security, so must the UK's appreciation of the scale of this threat grow.

Combined risks: everything, everywhere, all at once

63. In reality, few of the ten key threats we set out here will present as 'lone riders'; rather, several threats will present simultaneously. The interconnectedness of the modern economy generates the possibility that an adversary would combine different methods of attack, across different sectors, to amplify its effect. Jen Easterly, former head of the US' Cybersecurity and Infrastructure Security Agency, described this as "everything, everywhere, all at once".[102]

99 "Foreign states targeting UK universities, M15 warns", BBC News, 26 April 2025
100 "Russia tried to assassinate CEO of German arms firm sending weapons to Ukraine, reports say", Reuters, 11 July 2024
101 Q23
102 Q214; Select Committee on the Chinese Communist Party, Select Committee on CCP holds hearing on CCP cyber threat to American Homeland, 31 January 2024

64. Ciaran Martin, former CEO of the National Cyber Security Centre, used the example of "dozens or hundreds" of cyber-attacks on the UK's critical national infrastructure (CNI) "happening at the same time".[103] Amongst the "potential effects of war on the UK's way of life", set out in the Strategic Defence Review, are increased sabotage and cyber-attacks affecting critical national infrastructure (CNI), attempts to disrupt the UK economy, and efforts to manipulate information to undermine social cohesion and political will.[104] Lord Sedwill, former National Security Advisor, said that these attacks are "simply harder to respond to": "A combined cyber and information propaganda attack, for example, could be designed to disrupt essential supplies, create panic buying and affect public order…A sort of hybrid attack of that kind is extremely challenging to defend against and prepare for".[105]

65. Most of the UK's economy is privately owned and therefore the Government has limited means to directly intervene in its operation when emergencies arise, or in building resilience to risks before they become real. The Civil Contingencies Act 2004 provides for Ministers to take emergency powers in event of a catastrophic emergency, which would allow the Government to intervene directly, for example by overriding property rights.[106] However, this legislation has never been invoked, and the Government has recognised that it currently has "few legislative means through which to deliver rapid, non-consensual interventions in the case of company behaviour which may give rise to an emergency".[107]

66. Ciaran Martin told us that the UK's response to major incidents is largely dependent upon cooperation between Government and the private sector. While he said that this approach generally worked well, one area of particular concern was "where does the corporate interest stop and the public interest begin?".[108] For example, following a cyberattack on a private firm, what would be the level of required public impact for the response to become the Government's responsibility? Jamie MacColl, Senior Research Fellow at RUSI, echoed these concerns: "How is the British state preparing for a crisis or conflict scenario with another state, and what regulatory mechanisms is it creating to give us much more direct control of parts of the cyber-security of critical national infrastructure in a conflict scenario?"[109]

---

103 Q214
104 Ministry of Defence, The Strategic Defence Review 2025 - Making Britain Safer: secure at home, strong abroad, 2 June 2025
105 Q38
106 The Civil Contingencies Act 2004, s22
107 Cabinet Office, UK Government Resilience Action Plan, 8 July 2025
108 Q221
109 Q225

67. Businesses told us that there is currently no space, or institution, in which the public and private sectors can war-game and plan their response to the threats which the UK now confronts. Archie Norman, Chairman of M&S, called for the Government to make greater use of its "convening power": "If we are all invited to rock up and talk about cyber-security and national resilience, we will do so, and we will want to support".[110]

68. We questioned the then Chancellor of the Duchy of Lancaster about these concerns. He said that the Government's approach is guided by thinking through its response to all of the risks set out in the National Risk Register.[111] This tool only assesses the likelihood and impact of each risk individually. The recently published chronic risks analysis, the UK Government's first risk assessment for medium to long term risks, does provide some analysis of how chronic and acute risks, such as state threats and the vulnerabilities of global supply chains, might combine.[112] The Government has also committed to carrying out annual national exercises, known as the National Exercising Programme: simulations of a crisis designed to test the UK's capability to manage these emergencies.[113] Industry will be involved "in every phase of exercising".[114] It is unclear whether this will model responses to combined threats, or focus on singular events.

69. **CONCLUSION**

The ten key threats we outline above will rarely, if ever, present in isolation. Hostile actors are expected to target the UK economy along multiple vectors simultaneously. This poses particular challenges for an economy characterised by the private ownership of public risk, where the Government often lacks the tools to intervene rapidly across multiple sectors in response to a complex threat.

110 Q190. See Chapter 4 for further consideration of how to improve public-private intelligence sharing.
111 Q309
112 Cabinet Office, Chronic risks analysis, 8 July 2025
113 Cabinet Office, UK Government Resilience Action Plan, 14 July 2025, para 72
114 See previous reference

70. **CONCLUSION**

We have heard through this inquiry that there is currently no shared space for industry and Government to simulate their response to combined attacks across multiple sectors, or to plan public and private investments that improve long-term resilience. This is dangerous. The National Exercising Programme, if implemented correctly over the course of this Parliament, is a step in the right direction. However, it is important that these exercises do not solely model the response to singular risks, but that to multiple simultaneous modes of attack. It is only through stress-testing complex simulations that vulnerabilities across the public and private sectors can be identified and addressed.

71. **RECOMMENDATION**

The Government should conduct annual cross public sector-private sector exercises to specifically test the response to events in which multiple economic security risks manifest simultaneously. One example would be the scenario set out in the Strategic Defence Review: efforts to manipulate information, attacks on critical infrastructure, and wider attempts to disrupt the UK economy. These exercises could either form part of the National Exercising Programme or take place as a stand-alone wargame programme.

3 Transforming the economic security toolkit

72. We have now considered the main threats facing the UK's economic security, and the strategic principles that should underly the Government's response. There is however no single mechanism or policy that can translate strategic principles into action; the UK Government influences economic security through law, policy and a range of other levers. For ease of reference, we have described this collection of mechanisms as the UK's economic security "toolkit".

73. As economic security pervades every aspect of a nation's economy, an exhaustive list of every single Government lever that might safeguard economic security would be unwieldy and analytically unhelpful. In this baseline assessment, we have therefore focussed on seven sets of tools which are common in economic security discussions:

- Overarching government approach (definition; strategy/law; governance);
- Sanctions (financial and trade);
- Investment screening;
- Export controls (on military and dual-use items);
- Supply chains;
- Critical minerals; and
- Emerging technologies and cyber security.

74. In this chapter, we consider the UK's overall approach to economic security in comparison with toolkits available to the UK's allies. In the subsequent chapters, we will set out how individual elements of the UK's toolkit should be mobilised to deliver against our '6Ds' set of strategic principles.

The UK's toolkit in context

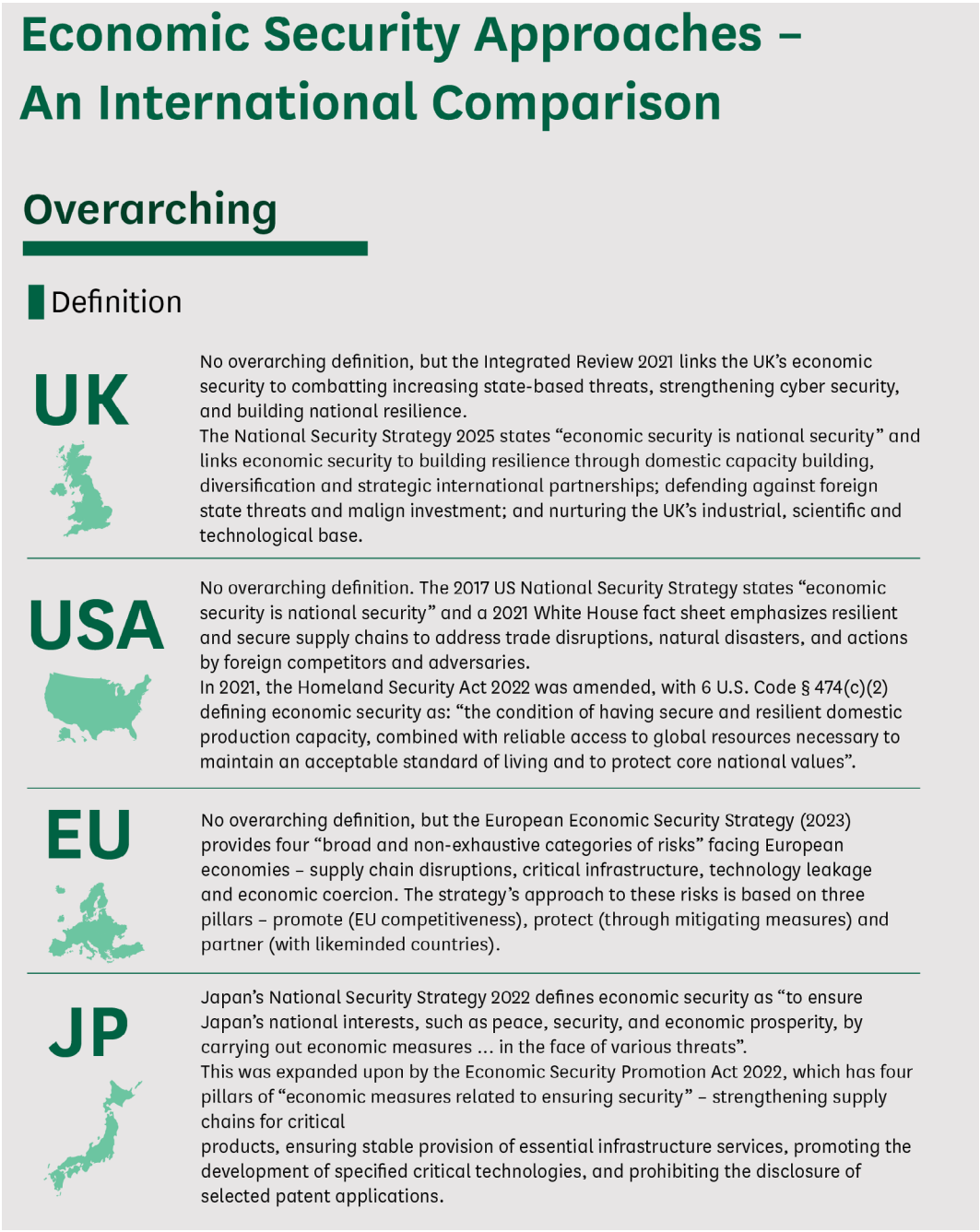
75. The threats outlined in Chapter 2 are not unique to the UK. As the world becomes more unstable and multipolar, many countries are thinking about how to improve their economic resilience or use economic weapons offensively.

76. The UK can, and must, learn from partners and allies for two reasons:

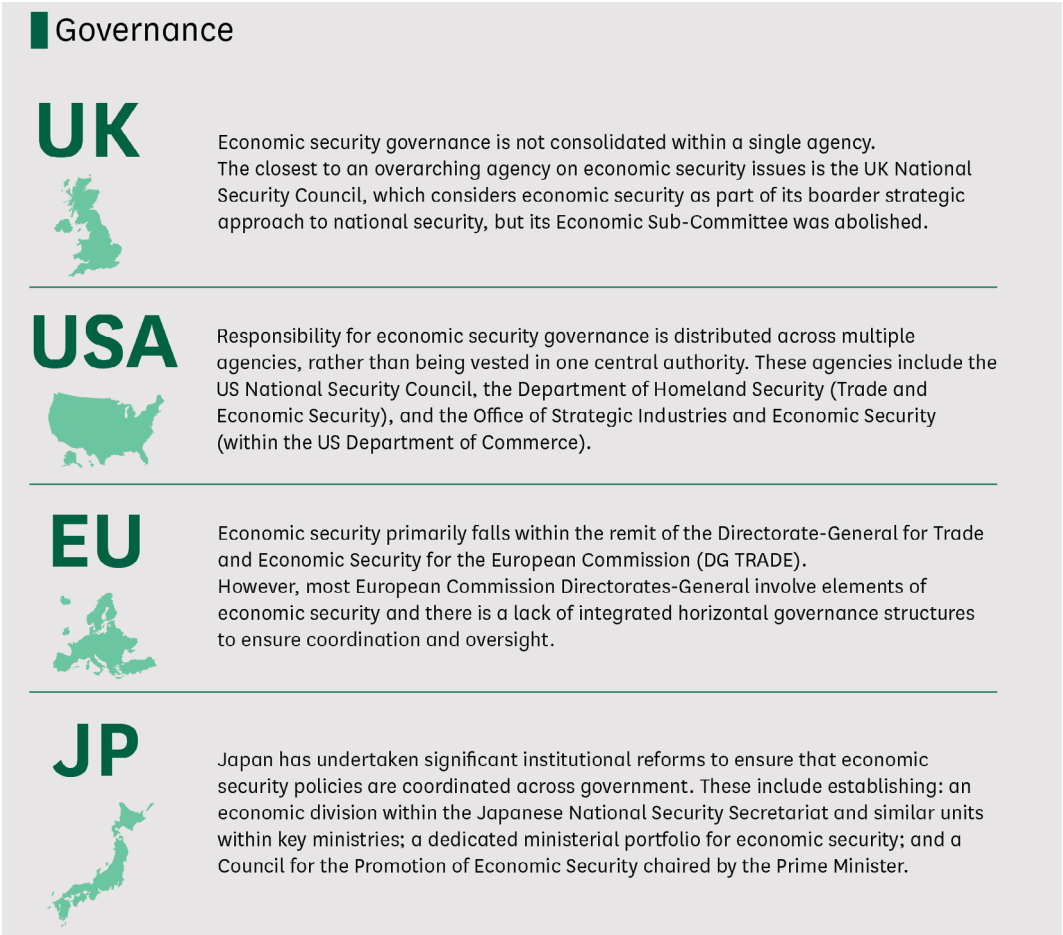
- First, there is no monopoly on wisdom, and the UK should actively seek to learn from best practice to improve the effectiveness and resilience of its economic security toolkit.
- Second, the UK must identify opportunities to align its economic security approach with those of likeminded countries. This effort, however, can only be based upon an understanding of how allies are tackling the challenges to their economic security, and where aligning strategy can produce a multiplier effect. The aim should be to ensure that the UK's economic security toolkit enhances (and is enhanced by) the resilience of a community of liberal, democratic, free-trading nations.

77. To ensure an up-to-date picture, we asked defence and security think tank RUSI to produce a comparative analysis of the UK's toolkit alongside the European Union, Japan and the US. RUSI's analysis is presented in Fig 1 below. This evidence complemented the evidence gathered on visits undertaken by the Committee to each of these jurisdictions in 2025. A brief summary of these visits is presented in Annex 1.

Fig.1: Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)



Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)



Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)

Regimes

Sanctions (financial and trade)

UK

The UK financial and trade sanctions regime is administered through a combination of specialized bodies with distinct responsibilities.
The Office of Financial Sanctions Implementation (OFSI), based in HM Treasury, oversees financial sanctions policy and enforcement, and has a Memorandum of Understanding with the US OFAC to support international coordination.
On the trade side, the Office of Trade Sanctions Implementation (OTSI) provides guidance to businesses and undertakes certain civil enforcement functions, while HM Revenue & Customs leads on the criminal enforcement of trade sanctions breaches.

USA

The US financial and trade sanctions regime is structured across several key agencies with complementary mandates.
The Office of Economic Sanctions Policy and Implementation in the US State Department develops and coordinates sanctions, while the Office of Foreign Assets Control (OFAC) in the US Treasury Department administers and enforces the majority of US financial and trade sanctions. OFAC has a Memorandum of Understanding with the UK OFSI to support transatlantic coordination.
The US Department of Justice National Security Division plays a critical role in prosecuting sanctions and export control violations, alongside broader national security offenses such as terrorism, espionage, and cybercrime.

EU

EU sanctions are proposed by EU member states and agreed by the EU Council on a unanimous basis (covers all forms of so-called 'restrictive measures'). Trade-related restrictions in the form of tariffs are imposed directly by the EU with no need for unanimity.
Whilst sanctions are imposed at the EU level, implementation and enforcement is the responsibility of individual member states.
Enforcement has recently been harmonized across the EU via Directive (EU) 2024/1226 on criminalizing sanctions evasion. The Directive came into force in mid-2024 and member states had to transpose it into their national law by May 2025, yet not all member states have done so – something the EU Commission has taken steps to enforce.

JP

Japan's financial and trade sanctions regime is primarily coordinated through the Ministry of Foreign Affairs, which designs and administers sanctions as a tool of foreign policy, and the Ministry of Finance, which is responsible for the implementation of financial restrictions.
Enforcement responsibilities are shared with other authorities, such as customs and law enforcement agencies, particularly for investigating and prosecuting sanctions breaches.

Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)

Investment screening (inbound and outbound)

UK

The UK's investment screening regime is anchored in the National Security and Investment Act 2021 (NSIA) that establishes a framework for reviewing both inbound and outbound investment on national security grounds.
For inbound transactions, the NSIA introduced mandatory notification requirements for acquisitions in sensitive sectors. A statutory review published in 2024 found the regime was broadly achieving its objectives. A public consultation launched July 2025 will review which activities fall under mandatory notification.
The NSIA also extends, in certain circumstances, to outward direct investment, such as where a proposed joint venture or acquisition involves an entity that carries out activities, provides goods or services in the UK, or has a UK connection.

USA

The US's investment screening regime covers both inbound and outbound investment, with distinct mechanisms for each.
The Committee on Foreign Investment in the United States – supplemented by the Foreign Investment Risk Review Modernization Act – reviews foreign acquisitions and investments that could pose national security risks. In parallel, the US Defense Department operates the Trusted Capital Marketplace, which connects vetted small and medium-sized technology providers with 'trusted' US capital.
The US Outbound Investment Security Program introduces a framework for screening certain US investments abroad to prevent the transfer of sensitive capital, expertise, or technology to strategic competitors.

EU

The EU's investment screening regime is evolving to address both inbound and outbound investment risks.
On the inbound side, the EU Foreign Direct Investment Regulation established a cooperation mechanism that allows the European Commission and member states to exchange information and raise concerns about foreign investments that may affect security or public order, while leaving final screening decisions to national authorities.
Building on this, in January 2025 the European Commission issued Recommendation (EU) 2025/63 urging member states to introduce mechanisms for screening outbound investment in sensitive sectors, such as semiconductors and quantum technologies.

JP

Japan's investment screening regime applies to both inbound and outbound investment, with tailored rules for each.
For inbound investment, the Cabinet Order on Inward Direct Investment requires prior notification and screening of foreign acquisitions in designated sensitive sectors, particularly where national security, public order, or the protection of critical technologies could be affected.
For outbound investment, the Foreign Exchange and Foreign Trade Act enables the government to regulate and restrict certain overseas transactions by Japanese entities, especially where such activities may pose risks to Japan's security interests or give foreign investors access to sensitive technologies or information.

Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)

Export controls (military, traditional, dual-use and advanced tech)

UK

The UK's export controls regime is administered by the Department for Business and Trade, with enforcement led by HM Revenue & Customs.
The primary legal framework comprises the Export Control Act 2002 and the Customs and Excise Management Act 1979, alongside secondary legislation, including the assimilated Dual-Use Regulation (EC) No. 428/2009 (that provides the main list of dual-use items and highly sensitive items), and the Export Control Order 2008 (that sets out controls on military items, additional dual-use and end-use controls, licensing and enforcement).
The Export Control Joint Unit assesses goods, software and technology against the UK Strategic Export Control Lists and other criteria to determine if licences should be granted.

USA

Responsibility for the US's export controls regime is divided across two primary authorities.
The Directorate of Defense Trade Controls, within the US Department of State, administers the International Traffic in Arms Regulations, which govern the export of defence articles, services, and related technical data listed on the US Munitions List.
The Bureau of Industry and Security, within the US Department of Commerce, oversees the Export Administration Regulations, which apply to dual-use items, sensitive technologies, and commercial products with potential military applications as set out in the Commerce Control List.

EU

The central legal framework for EU export controls is Regulation (EU) 2021/821, which provides a list of dual- use items and establishes end-use controls on non-listed items, as well as controls on brokering, technical assistance and transit dual-use goods.
The EU maintains a common list of military items (e.g. weapons, ammunition, firearms, software, technology and equipment "specially designed or modified for military use"). However, enforcement of export controls takes place at the national level, which results in variation in how the controls are applied.
In April 2025, the European Commission issued Recommendation (EU) 2025/683 aimed at improving the coordination of national export controls for dual-use goods.

JP

Japan's export controls regime is anchored in the Foreign Exchange and Foreign Trade Act (FEFTA).
FEFTA does not specify which goods or technologies require licences but is implemented through two Cabinet Orders: the Export Trade Control Order (for goods) and the Foreign Exchange Order (for technology and software). These create two control categories: (i) List Controls, covering conventional weapons and items with weapons of mass destruction potential; and (ii) Catch-All Controls, which apply to non- listed items when their end use or user raises security concerns, such as entities on the End User List.
In 2024, Japan added semiconductors and quantum computers to List Controls, and major changes to Catch-All Controls will take effect in October 2025.

Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)

Supply chains

UK

The UK Critical Imports and Supply Chain Strategy (2024) complements the wider Industrial Strategy 2025, which is supported by Sector Plans for 8 critical industries, as well as the government's Trade Strategy 2025.
The Industrial Strategy 2025 plans to expand institutional capacity by creating a Supply Chain Centre by the end of 2025 to monitor vulnerabilities and coordinate responses.
To support the private sector, the National Cyber Security Centre has published supply chain security guidance, and the Trade Strategy 2025 announced the Department for Business and Trade will launch an Economic Security Advisory Service, offering guidance to businesses on navigating supply chain risks and aligning business with the UK's broader economic security agenda.

USA

Recent measures have included executive actions to strengthen domestic production capacity (see the critical minerals section below), targeted investments under industrial and infrastructure programs, and expanded cooperation with allies on shared vulnerabilities (e.g. the Australia-UK-US Supply Chain Resilience Cooperation Group).
A major legislative development is the Promoting Resilient Supply Chains Act of 2025, which has passed the House of Representatives but has not yet become law. If enacted, it would provide a statutory basis for enhanced federal coordination, monitoring of critical dependencies, and initiatives to diversify sourcing and strengthen partnerships with the private sector.

EU

The European Economic Security Strategy (EESS) sets out measures to safeguard the EU's technological and industrial base, reduce strategic dependencies, and reinforce the resilience of critical supply chains.
As part of this framework, the European Commission has initiated regular economic security risk assessments, which identify vulnerabilities and "supply chain distress" across key sectors to inform coordinated responses at both the EU and member-state level. These risk assessments have so far focused on four critical technology areas that were deemed to present immediate risk, and sit alongside continuing risk assessments identified in the EESS relating to the resilience of supply chains, physical and cyber security of critical infrastructure, and economic coercion.

JP

Domestically, the Economic Security Promotion Act provides the foundation for a comprehensive economic security strategy, equipping the government with the tools to strengthen supply chains in strategic sectors and reduce vulnerabilities.
Internationally, Japan has taken a leading role in regional initiatives such as the Supply Chain Resilience Initiative with Australia and India, which promotes reducing trade dependency on China via supply chain diversification, and the Indo- Pacific Economic Framework, which establishes mechanisms for mutual support and coordination during supply chain disruptions.

Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)

Critical minerals

UK

The UK's Critical Minerals Strategy was first published in 2022 and is being revised to reflect evolving supply chain and security priorities.
The strategy sets out how the UK intends to secure reliable access to critical minerals essential for advanced technologies and the green transition. International partnerships are a key feature, including the UK–Japan Critical Minerals Memorandum of Cooperation, which promotes collaboration on resilient, transparent and sustainable critical mineral supply chains.
Domestically, the UK Critical Minerals Intelligence Centre provides analysis and data that inform policy development, including inputs into sector definitions under the National Security and Investment Act 2021.

USA

The US does not currently have an overarching critical minerals strategy or Act (although the US Department of Energy has a strategy and maintains a list of designated critical minerals). Instead, it tends to operate through targeted executive actions and bilateral agreements.
For instance, Executive Order 14241 (Immediate Measures to Increase American Mineral Production) and Executive Order 14152 (Unleashing American Energy) increase the US's production and processing of critical minerals on an accelerated timeline, supported by significant public and private capital.
In addition to domestic initiatives, the US has prioritised bilateral partnerships to secure supply chains, most notably through the US-Japan Critical Minerals Agreement and the announced US/Ukraine deal.

EU

The EU's critical minerals regime is governed by the Critical Raw Materials Act (CRMA), which establishes a framework to strengthen supply chain resilience and reduce dependencies. A key element is the designation of 47 Strategic Projects, representing around €22.5 billion in investment, aimed at boosting extraction, processing and recycling capacity across the bloc.
The CRMA is closely tied to the Green Deal Industrial Plan, to ensure secure access to raw materials needed for clean technologies and green transition competitiveness.
Internationally, the EU has pursued strategic partnerships, including the EU-Japan Administrative Arrangement on Cooperation in Critical Raw Materials Supply Chains, to reinforce diversification and sustainability of supply.

JP

Japan's critical minerals regime is governed by the Economic Security Promotion Act (ESPA) and the government's designation of "Specified Critical Products", including key critical minerals essential for advanced manufacturing and clean energy technologies.
The ESPA provides a legal framework for securing supply chains through state support, stockpiling, and diversification measures.
International cooperation forms a central pillar of Japan's approach: the US agreement underpins bilateral collaboration on sustainable sourcing and secure trade, while the UK and EU agreements strengthen efforts to enhance supply chain resilience.

Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)

Emerging technologies

UK

The UK Industrial Strategy 2025 is supported by Sector Plans for 8 critical industries. The Digital and Technologies Sector Plan identifies 6 "frontier technologies": advanced connective technologies, artificial intelligence (AI), cyber security, engineering biology, quantum technologies and semiconductors. This overarching framework is reinforced by dedicated national strategies for the individual technologies.
UK analysis has found the convergence of existing and emerging technologies has complex economic impacts and cyber security implications. Work at this intersection includes cyber security sectoral analysis, Cyber Growth Action Plan 2025, and the forthcoming Cyber Security and Resilience Bill and refreshed National Cyber Strategy.

USA

The National Science and Technology Council maintains a Critical and Emerging Technologies List, to guide federal and agency-level priorities. The technologies identified include advanced computing, AI, biotech, navigation, data and cybersecurity, quantum and semiconductors.
The US's approach to these technologies combines significant subsidies and research funding (e.g. $280 billion under the CHIPS and Science Act 2022) with the removal of regulatory barriers (e.g. America's AI Action Plan and linked executive orders).
US strategic direction has also been set by the National Strategy for Critical and Emerging Technology 2020 and National Cybersecurity Strategy 2023, which integrate emerging technologies with cybersecurity.

EU

Under the European Economic Security Strategy (EESS), the European Commission identifies 4 critical technology areas that present urgent economic security risks: AI, quantum, semiconductors and biotechnologies. These areas have been the subject of the first EESS in-depth risk assessments designed to inform mitigation measures.
EU legislative, investment and research initiatives such as the AI Act, European Chips Act, Strategic Technologies for Europe Platform, European Strategy on Research and Technology Infrastructures, and Quantum Europe Strategy underpin EU ambitions to reduce external dependencies while advancing competitiveness and innovation. The EU ties tech growth to cyber security, through its Cybersecurity Strategy and Digital Decade policy programme.

JP

Japan's Economic Security Promotion Act provides protection and support for "Specified Critical Products", which include emerging technologies, such as semiconductors, industrial robots and cloud services.
Initiatives such as the Semiconductor and Digital Industry Strategy and the AI and Semiconductor Industry Enhancement Framework aim to stimulate over ¥50 trillion in public and private investment in Japanese technological innovation by 2030 – ensuring stable supply chains while also embedding ethical standards.
In May 2025, Japan passed its first AI legislation and modernised its cyber security framework. Both are designed to secure Japan's technological advantage while protecting against risks in the digital domain.

Comparison of economic security approaches, based on evidence submitted by Centre for Finance & Security, RUSI (ECO0036)

78. **CONCLUSION**

The evidence we have received, and a comparison with our allies, leads us to conclude that the UK's economic security regime is no longer fit for the future. A whole-of-society approach must become the organising principle of Britain's economic security.

Improving cross-Government coordination

79. RUSI's comparative analysis suggests that a key difference between the UK and its allies is the UK's dependence on a collection of policy documents, rather than an overarching legislative and institutional framework. RUSI argued that the UK's reliance on strategies for individual elements of economic security, such as the Trade Strategy or the Industrial Strategy, means that our approach is vulnerable to "political turnover" and discontinuity.[115] RUSI contrasted this with the legislative frameworks in Japan and the United States which provide continuity beyond electoral cycles, enabling long-term industry and investor confidence.[116]

80. Submitters also argued that this reliance on a library of individual strategies risks undermining cross-Government coordination. ADS Group told us that there is a risk that the UK's various strategies pay "lip service to the issue from siloed positions".[117] RAND Europe argued that, absent a clear overarching framework, departments may end up "pursuing diverging objectives".[118]

81. Evidence we received argued that institutional reform was also key to a more coherent whole-of-Government approach. Lord Sedwill told us that the UK Government is "naturally siloed" with "vertical structures... much stronger than every attempt to burrow across them with horizontal connecting tissue."[119] He argued that effective economic security policymaking requires the creation of "strong, not just co-ordinating but integrating, machinery...in order to get everyone lined up and pursuing a common strategy".[120] Likewise, Professor Jonathan Boff called for the establishment of an 'Economic Security Organisation' which would "bring together relevant stakeholders from all across Whitehall" and consider UK strategy in the round.[121]

82. Japan has undertaken various institutional reforms to "ensure that economic security policies are coordinated and consistent across government", in the words of RUSI.[122] This included establishing an Economic Security Unit within the Japanese National Security Secretariat, a dedicated ministerial portfolio for economic security, and a Council for the

115 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0036)
116 See previous reference
117 ADS Group (ECO0002)
118 RAND Europe (ECO0021)
119 Q59
120 See previous reference
121 Professor Jonathan Boff (Professor of Military History at University of Birmingham) (ECO0008)
122 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0036)

Promotion of Economic Security chaired by the Prime Minister. The Centre for Inclusive Trade Policy and the UK Trade Policy Observatory highlighted the importance of the Council in facilitating "cross-departmental coordination" across the Japanese government.[123]

83. In the aftermath of World War I, the UK implemented a similar series of institutional reforms to create a 'fourth fighting service' and to facilitate intra-Whitehall collaboration on economic security related issues.[124] In 1923, the UK Government established the Advisory Committee on Trade and Blockade in Time of War (ATB) to capture the lessons from the UK's experience of economic warfare, coordinate the collation of economic intelligence, and plan the necessary machinery and legislation required for a future economic war.[125] Professor Jonathan Boff highlighted the ATB's success in operating as a "forum for intra-Whitehall thinking and debate about economic statecraft", accelerating and improving subsequent decision-making during World War II. The ATB also drew up plans for the 'Ministry of Economic Warfare' (created to wage economic war against the Axis Powers), enabling this department to be stood up quickly following the outbreak of war.[126]

84. Today, according to RUSI, the "closest to an overarching agency on economic security issues" in the UK is the National Security Council (NSC).[127] The NSC is the UK Government's main forum for collective discussion of its objectives for national security - but its Economic Security Sub-Committee was abolished in July 2024. Since then, the Government has said that the NSC "considers economic security, as parts of its broader strategic approach to national security".[128] The Secretary of State for Business and Trade, however, is no longer a permanent member of the NSC.[129]

85. When asked, the then Minister of State for Trade Policy and Economic Security Douglas Alexander said his role as a joint minister - working across both the Department for Business and Trade and the Cabinet Office - significantly improved cross-Government coordination. He told us that it had made "a very material difference to the functioning of not just our

123 Centre for Inclusive Trade Policy and UK Trade Policy Observatory (ECO0014)
124 See Jack Connolly, 'The Fourth Fighting Service': The early development of British Economic Statecraft (PDF), Blavatnik School of Government, January 2024.
125 Professor Jonathan Boff (Professor of Military History at University of Birmingham) (ECO0008). See also, Jack Connolly, 'The Fourth Fighting Service': The early development of British Economic Statecraft (PDF), Blavatnik School of Government, January 2024
126 Professor Jonathan Boff (Professor of Military History at University of Birmingham) (ECO0008)
127 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0036)
128 National Security Council PQ 11829, 4 November 2024
129 Cabinet Office, List of Cabinet Committees and their membership (accessed 11 November 2025)

relationships but our effectiveness across Government".[130] Following the September 2025 reshuffle, however, this joint role in its previous form was abolished. Sir Chris Bryant, Minister of State for Trade Policy, maintains responsibility for 'economic security'. Unlike Douglas Alexander, however, Sir Chris no longer sits across both the Department for Business and Trade and the Cabinet Office.[131]

86. **CONCLUSION**

The UK's approach to economic security shows less cross-government co-ordination than our most important international partners. The Government's approach is characterised by siloed thinking, a lack of adequate institutional support, and a reliance on strategies that are vulnerable to churn as ministers and governments change. The abolition of the National Security Council's Economic Security Sub-Committee leaves even less clarity as to how economic security will be factored in at the heart of Government decision-making.

87. **RECOMMENDATION**

The Government must urgently reform Whitehall structures to improve cross-government co-ordination of economic security policy. We recommend that the Government learn from its own history, and following from the example of the 1920s it should:

- Appoint a cross-Government Minister for Economic Security, based in the Cabinet Office. This Minister should have responsibility for coordinating economic security related policy across Government, and be made a permanent member of both the National Security Council and the Economic Security sub-committee.
- Establish a new Office of Economic Security, that would bring together relevant expertise from across Whitehall, provide a platform for coordination with the private sector, and monitor the overall effectiveness of the UK's toolkit.
- Reinstate the Economic Security sub-committee of the National Security Council, with the Minister for Economic Security and the Secretary of State for Business and Trade as permanent members.
- Introduce legislation which would implement the recommendations of this report, and put the economic security related components of pre-existing strategies onto a statutory footing.

130 Q286

131 GOV.UK, Minister of State (Minister for Trade), Sir Chris Bryant MP (accessed 17 October 2025)

If the Government rejects the implementation of these measures, we recommend that it sets out in writing how it will improve cross-Government coordination, and ensure that its approach is driven by long-term goals.

The role of Parliament

88. Parliament has scrutinised economic security through various channels in recent years. The Joint Committee on the National Security Strategy (JCNSS) opened an inquiry into the UK's economic security in the 2019–24 Parliament, but had not produced a report before the 2024 General Election was called. Our Committee's predecessor in that Parliament also established a Sub-Committee on National Security and Investment, which took evidence on the UK's investment screening regime and provided a response to the then-Government's call for evidence on the National Security and Investment Act 2021.

89. A fundamental role of Parliament, and the select committee system in particular, is the scrutiny of Government decision-making. Parliament will therefore have a vital role monitoring the Government's progress in improving cross-Government coordination.

90. However, our predecessor Committee was long concerned by barriers that limit Parliament's ability to scrutinise government effectively. The UK's investment screening regime, for instance, is set out in the National Security and Investment Act 2021 (NSIA). In February 2024, our predecessor Committee said that the design of the NSIA was prohibiting Parliament from accessing necessary information about the ways in which decisions were taken on individual cases. Specifically, section 54 of the NSIA prevents the Government from sharing with Parliament any information received from third parties under the Act.[132] Our predecessor Committee called on the previous Government to explore ways of amending section 54 to enable it to adequately scrutinise the efficacy of this legislation. This was rejected by the previous Government on the basis that it and the Committee had agreed

132 Business and Trade Sub-Committee on National Security and Investment, Business and Trade Subcommittee response to the Call for Evidence on the National Security and Investment Act 2021 (PDF), 9 February 2024. Section 54(2) of the Act lists a narrow set of reasons for disclosing information to public authorities and facilitating parliamentary scrutiny is not among them. In addition, the NSI Act makes clear that "public authority" has the same meaning as in section 6 of the Human Rights Act 1998'; this does not include either House of Parliament.

that its role in scrutinising individual cases would be 'exceptional' rather than 'routine'. The then Government also noted that such a change would require primary legislation, which it was not considering.[133]

91. **CONCLUSION**
Parliament and its committees must play a leading part in the national discussion around economic security, convening stakeholders from across sectors and advising Government on the strategic and cross-cutting steps needed to confront its challenges. Parliament, however, cannot hold the Government to account on its overall strategy for economic security if it is not able to access key information about the use of the UK's toolkit.

92. **RECOMMENDATION**
The Government should commit to supporting select committee scrutiny of its approach to economic security. This should include a commitment to at least biannual public evidence sessions with senior Ministers and officials, and to complying with all reasonable requests for written information. This should include regular and comprehensive reports on the operation of the UK's economic security enforcement regimes, including sanctions, investment screening and export controls.

93. **RECOMMENDATION**
We acknowledge that some information may need to be provided in confidence, and we invite a dialogue between Government and Parliament to determine the appropriate parameters for this.

94. **RECOMMENDATION**
We reiterate the recommendation of our predecessor Committee, and recommend the Government explore ways of amending section 54 of the National Security and Investment Act 2021 to enable information relating to investment screening decisions to be shared with Parliament.

Reforming the toolkit

95. Establishing a whole-of-government approach to economic security is a necessary step toward building the UK's resilience, but it is only the first step. The remaining Chapters of this Report set out how we believe individual elements of the UK toolkit should be reformed, to integrate a whole-of-society approach where Government and industry both have vital roles to play.

133 Cabinet Office, Government response to the Business and Trade Committee's submission to the National Security and Investment Act Call for Evidence 2023, 18 April 2024

4 Diagnose a shared understanding of threats

96. Achieving a 'whole of society approach' to economic security will require a shared diagnosis of the threats the UK faces across the public and private sectors.

97. It is not a given that public and private perceptions of 'risk', including threats, align. Governments, through their national security apparatus, assess the threats to their own individual jurisdictions. The doctrine of shareholder primacy means that the allegiance of a Western private company is not to a country, but to its shareholders. For a multinational, this might entail making cost-benefit trade-offs on resilience on a global basis, rather than necessarily applying a county-level perspective.

98. Government has access to sources of intelligence about emerging threats that are not available to private organisations. Without this intelligence, firms must weigh security and political risks - such the stability of the countries where their suppliers operate - without knowing the Government's private concerns.[134] While the confidential nature of government intelligence can create barriers to sharing information with privately run organisations, our evidence suggests that the Government needs to go much further in the information it is prepared to disclose. This is particularly the case for intelligence that would enable businesses to identify and understand the risks arising from state action.[135]

99. Evidence highlighted the National Cyber Security Centre (NCSC) as an example of best practice in public-private information sharing. Sir Simon Fraser described the NCSC as a "very successful example" of how "quite sensitive information that is held in relatively secret parts of Government can be effectively shared in a responsible and controlled way".[136]

100. Steps were taken in the previous Parliament to replicate this model in the economic security domain. For instance, the Economic Security Public-Private forum was created in 2023. At this forum, chaired by the then Deputy

134 Joint Committee on the National Security Strategy, Oral evidence: The UK's economic security, 26 February 2024, Q29

135 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0012). See also Q24

136 Q29

Prime Minister, attendees from 11 businesses (across the "most strategically important sectors of the UK economy") received a declassified quarterly economic security briefing from the National Protective Security Authority.[137] This initiative has not been mentioned in any recently published policy documents, such as the Trade Strategy.

101. The evidence suggests, however, that more effective intelligence-sharing by itself will not necessarily align the public and private sector in their understanding of risk. Alexandra Kellert, Associate Director at Control Risks, a London-based global risk consultancy, told us that threat briefings will only be useful for industry if they "can be framed in a way that has practical impacts" for businesses.[138]

102. We heard that business-to-business forums can play a key role in filling this gap. Katharina Sommer, Group Head of Government Affairs and Analyst Relations at the cyber security firm NCC Group, speaking in the context of cyber security, told us that "more mature private sector partners, whether they come from the cyber industry or from businesses" can act as the "bridge" between Government and other firms: "We'll do that translation layer and make that intelligence actionable for a less mature organisation."[139]

103. Witnesses made clear that improving industry collaboration will require greater support from the Government. Dominic Kendal-Ward, Group Secretary and General Counsel at the Co-op Group, told us that very often legal or competition considerations create "nervousness" around sharing information. He said that the Government can play an important role in "creating those safe spaces" to more candidly share learnings and intelligence.[140] Archie Norman, Chairman of M&S, called on Government to "play a bigger role" in making sure that lessons from serious incidents are socialised amongst a larger number of organisations.[141]

104. The Government has recognised that its current engagement with businesses on economic security issues is "too complicated and disparate".[142] To this end, the Trade Strategy announced a new Economic Security Advisory Service, offering advice, guidance and support to businesses on economic security risks and threats. When we asked Douglas Alexander, then Minister for Trade Policy and Economic Security, about his ambitions for the service, he said that it would provide a "a clearer portal

137 Cabinet Office, Deputy Prime Minister and Business Secretary join business leaders for "first of its kind" declassified economic security briefing, 13 December 2023
138 Q30
139 Q228
140 Q210
141 Q187
142 Department for Business and Trade, The UK's Trade Strategy, 26 June 2025

and point of contact with Whitehall". He told us that this would include an "effective online offering" and "an effective brokering service", targeted at firms in the eight growth-driving sectors identified in the Industrial Strategy.[143]

105. **CONCLUSION**

The severity and breadth of the threats facing UK economic security will require a step change in information sharing between Government and the private sector. Businesses need accurate, up-to-date and actionable insights in order to plan investments and work constructively with government. We welcome the positive change that the new Economic Security Advisory Service could bring as a centre for advice, guidance and support to industry. However, it is essential that the Service does not operate solely as a Government-led initiative, but provides a forum for wider information sharing both between the public and private sectors, and within the private sector.

106. **RECOMMENDATION**

The Government should increase its ambitions for the Economic Security Advisory Service to ensure that it acts as a centre for collaboration and information-sharing. Alongside its proposed functions, its remit should also encompass:

- The functions of the previous Economic Security Public-Private Forum, with National Protective Security Authority (NPSA) briefings and research collaboration advice provided to businesses;
- Forums for businesses to discuss challenges and risks with both the Government, and other businesses, in order to share best practice and identify emerging threats; and
- A facility to provide tailored guidance and support regarding state-based threats.

We recommend that the Government follow, and build on, the example of the National Cyber Security Centre in facilitating effective public-private co-operation. This platform should be organised by the new Office of Economic Security.

143 Q270

Diagnosing the impacts of emerging technology

107. Our evidence also highlighted the importance of the UK's threat diagnosis keeping pace with technological advancement. Trade association techUK, a trade association for the UK technology sector, told us that emerging technologies can enable "huge new benefits and capabilities", while also generating "new threats to both national and economic security".[144] For instance, as set out in Chapter 2, the development of artificial intelligence can be used to both increase productivity, and enable sophisticated cyber-attacks. As a result, the Coalition on Secure Technology, an organisation campaigning to raise awareness of the risks of technology produced by hostile states, contended that the "distinction between civil and military uses of science and technology is being eroded".[145] It is therefore essential that the UK's toolkit evolves so that it can protect against the new risks arising from emerging technologies.

108. Currently, much of the Government's work in forecasting the threats involving emerging technologies takes place within individual departments or units. The Export Control Joint Unit, for instance, is reviewing the impact of emerging technologies on the UK's export control regime. The Investment Screening Unit, sitting within the Cabinet Office, uses its own process of technological forecasting to understand emerging sectors of concern. Steps were taken in the previous Parliament to improve cross-Whitehall understanding of emerging technology, such as through the establishment of the National Security Technology and Innovation Exchange (NSTIx). NSTIx was a unit working to improve collaboration across the Government's national security science, innovation and technology work. It was abolished in 2025, and its functions have been "taken forward within other national security teams".[146]

109. We were told that this decentralised approach means that the UK lacks a holistic understanding emerging technology's impact on its economic security toolkit. The Coalition on Secure Technology told us that coordination between departments on these issues was currently "poor".[147] They called for the establishment of a "coordinating body, a centre of expertise on science and technology security, to oversee planning and implementation of protective measures across government".[148] Trade

144 techUK (ECO0030)
145 Coalition on Secure Technology (ECO0015)
146 National Security Technology and Innovation Exchange PQ 41118, 1 April 2025
147 Coalition on Secure Technology (ECO0015)
148 See previous reference

association techUK highlighted the need for investment in greater cross-Government "technical and foresight expertise" to accurately assess and mitigate emerging risks.[149]

110. **CONCLUSION**
Emerging technologies have the potential to profoundly impact the UK's economic security. The UK's protective measures must keep pace with new risks, while not harming the competitiveness of its own technology sector. An accurate cross-Government understanding of the national security implications of future technologies will be essential, to mitigate harms and inform joined-up policymaking.

111. **RECOMMENDATION**
We recommend that the creation of a cross-Government technology forecasting unit. This would lead an annual technology forecasting process, to support a co-ordinated response to technological change and the risk of new harms across the UK's economic security toolkit. This unit should be based within the new Office of Economic Security, to provide a cross-Government liaison point.

149 techUK (ECO0030)

5 Develop sovereign capabilities

112. Growing geopolitical competition has heightened the risks associated with over-reliance on foreign suppliers, and led to an increased emphasis amongst policymakers on developing sovereign capabilities in critical sectors.

113. The 2025 National Security Strategy (NSS) sets out the UK's ambition to "increase sovereign and asymmetric capabilities".[150] These terms are not formally defined, but the NSS sets out three broad components:

- Rebuild the UK's core defence industrial base, primarily through the reforms to defence procurement set out in the Defence Industrial Strategy.
- Identify, protect and grow other sovereign capabilities that are key to the UK's industrial base. This is a wider ambition to protect the UK's "long-term competitiveness", through the plans to support and grow the eight sectors set out in the Industrial Strategy.
- Pursue 'asymmetric advantage'. This involves focussing on areas where the UK can gain an edge over other states, through strategically targeted investment in the research and development of frontier industries and technologies.

114. We have long been concerned as to the Government's lack of precision in defining these terms. In April 2025, as part of our Industrial Strategy inquiry, we submitted our proposals to the Government's consultation on its strategy for the steel industry. One of our tests for the strategy is that it sets out "a clear statement of the Government's 25–30 year vision for steel", including a statement of the steel capabilities that the UK needs onshore.[151] In the NSS, the Government describes the passage of the Steel Industry (Special Measures) Act 2025 as an example of the "more activist approach" it will take in protecting "sovereign capability".[152] However, it does not then

150 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

151 Letter from the Chair to the Secretary of State for Business and Trade relating to a plan for Steel (PDF), 1 April 2025

152 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

define the future role of the sector. Similarly, the Defence Industrial Strategy describes the sector as an area where action is needed to strengthen UK and allied capability, but does not set out what this means in practice.[153]

115. We wrote to the Government in June 2025 asking that the Defence Industrial Strategy contain clear definitions of the sovereign capabilities the UK seeks to on-shore, and the capabilities we are content to trade for.[154] The Defence Industrial Strategy confirms the 'National Security Priorities', such as nuclear submarines, where "strategic imperative requires full, or majority, industrial capability to be UK-based".[155] However, the desired level of 'sovereignty', for instance whether to onshore the entire supply chain as well as submarine production, remains unclear.

116. When we asked the then Chancellor of the Duchy of Lancaster to further define what sovereign capabilities the Government wants to curate, he told us that the starting point should be "to read the Industrial Strategy", and the eight growth driving sectors it sets out (the 'IS-8').[156] Douglas Alexander, the then Minister of State for Economic Security and Trade Policy, added to this the 'foundational sectors' set out in strategy: "electricity networks, ports, construction, steel, critical minerals, composites, materials and chemicals, all of which we regard as essential to support the IS-8 sectors".[157]

117. While submitters acknowledged the Industrial Strategy as a useful first step in defining the UK's economic strengths,[158] they called for the UK Government's approach to also be guided by an assessment of current areas of high dependency. Oxford China Policy Lab pointed to the UK's AI infrastructure as an example of an area where the UK "risks becoming reliant on foreign-produced AI models and infrastructure…[which] could leave the UK exposed to pressure over access or control of these technologies".[159] The announcement of the US-UK Tech Prosperity Deal in September 2025 led Dr Pia Hüsch and Sophie Williams-Dunning, writing for RUSI, to question how sovereign UK infrastructure is "if it is funded, designed, built, and operated by American companies?"[160]

153 Ministry of Defence, Defence Industrial Strategy 2025: Making Defence an Engine for Growth (PDF), 8 September 2025, p24
154 Letter from the Chair to the Secretaries of State for Business and Trade and Defence relating to the Defence Industrial Strategy (PDF), 18 June 2025
155 Ministry of Defence, Defence Industrial Strategy 2025: Making Defence an Engine for Growth (PDF), 8 September 2025, p24
156 Q267
157 Q268
158 RAND Europe (ECO0021)
159 Oxford China Policy Lab (ECO0016)
160 RUSI, A Big, Beautiful US Investment Boost for the UK Tech Sector, 26 September 2025

118. In order to accurately understand these possible dependencies, Oxford China Lab called for a wide-ranging evaluation of the "existing and emerging dependencies where UK reliance on foreign-owned networks and resources could be strategically cut or limited".[161] The Centre for Inclusive Trade Policy and UK Trade Policy Observatory called for this is to more broadly assess "important and key sectors".[162] Such an assessment, according to the Oxford China Lab, should also acknowledge "the UK's limitations in producing fully homegrown systems and networks, such as foundational critical digital infrastructures".[163]

119. Evidence received suggests that the development of sovereign alternatives requires clear long-term financial support from the Government. Professor Michael Lewis, Professor of Operations and Supply Management at the University of Bath, said that the necessary investment in these capabilities often contradicts "short-term economic logic". This is because the goal is not to necessarily create systems that "will be superior today, but [whose] absence represents strategic exposure tomorrow". He argued that the Government would need to provide "clear, consistent demand signals" to encourage private sector investment into the capabilities it identifies.[164] ADS Group told us that through investing strategically the Government can "anchor critical capabilities", encouraging private investment into these sectors, and increasing national resilience.[165]

120. The nature of public investment required to safeguard the nation's economic security is likely to require modernising the UK Government's standards for managing public resources set out in the Treasury's 'Managing Public Money' publication.[166] Accounting officers are required to scrutinise proposals according to four tests: regularity, propriety, value for money, and feasibility. They have a duty to then seek a 'ministerial direction' if they think a spending proposal breaches these criteria. Managing Public Money notes that often the circumstances giving rise to a direction are "novel, contentious, or repercussive".[167] Notwithstanding the ministerial direction process, there is no explicit provision in Managing Public Money for spending decisions to be based on economic security concerns.

121. The risks of this lacuna have already been highlighted on two occasions over the course of our inquiry. A ministerial direction was issued following the Government's decision to take control of the British Steel site at

161 Oxford China Policy Lab (ECO0016)
162 Centre for Inclusive Trade Policy and UK Trade Policy Observatory (ECO0014)
163 Oxford China Policy Lab (ECO0016)
164 Professor Michael Lewis (ECO0027)
165 ADS Group (ECO0002)
166 HM Treasury, Managing Public Money, June 2025
167 See previous reference

Scunthorpe[168] where the accounting officer said that the "speed" required of the transaction precluded the possibility of a full assessment.[169] As of 14 October 2025, the cost of implementing this measure stood at £235 million.[170] A second ministerial direction was issued following the cyber attack on Jaguar Land Rover (JLR), when the Government provided JLR with a guarantee for a £1.5 billion loan. UK Export Finance said that this loan would fall outside of its usual underwriting criteria.[171] The Secretary of State for Business and Trade, however, said that proceeding was in the "national interest", because JLR and its suppliers were major employers.[172] Given the threat landscape described in Chapter 2, there is little reason to suppose that incidents requiring such expenditure will diminish in the coming years.

122. Other jurisdictions have taken a more structured approach to defining sovereign capabilities. As set out in Fig 1, Japan's approach to sovereign capabilities combines both clarity as to the Japanese Government's priorities and financial support. Through Japan's Economic Security Promotion Act, the Government is able to designate certain goods as 'critical materials'. Examples include semiconductors, EV batteries, cloud services, and ship parts. The domestic manufacture of these goods is then encouraged through the subsidisation of companies in these sectors.

123. **CONCLUSION**
Economic security requires a clear-eyed understanding of which capabilities the UK needs to deliver for itself. Yet it is still not clear to us or, more importantly, to business investors what sovereign and asymmetric capabilities the Government aims to develop. So far, its approach has focussed on highlighting areas of economic strength, with no assessment of the areas in which it is over reliant on foreign-owned resources.

124. **CONCLUSION**
The development of these sovereign capabilities is likely require an approach to public expenditure that is novel and not reflected in UK Government accounting principles. These principles evolved in a different era when our economic security was less perilous.

168 Department for Business and Trade, Letter from the Secretary of State for Business and Trade to the Permanent Secretary (PDF), 12 April 2025
169 Department for Business and Trade, Letter from the Permanent Secretary to the Secretary of State for Business and Trade (PDF), 12 April 2025
170 British Steel, HCWS957, 14 October 2025
171 Department for Business and Trade, Letter from UKEF CEO Tim Reid to the Secretary of State setting out his position as Accounting Officer for UKEF (PDF), 25 September 2025
172 Department for Business and Trade, Letter from the Secretary of State to UKEF CEO Tim Reid acknowledging his position and setting out his direction for UKEF to provide a guarantee to Jaguar Land Rover (PDF), 26 September 2025

125. **RECOMMENDATION**
The Cabinet Office should work with relevant sector bodies and Departments, to identify and publish a list of the 'sovereign capabilities' the Government wishes to develop for the nation. We recommend that the Government learns lessons from the approach taken under Japan's Economic Security Promotion Act in developing the UK list. It should include both sectors of strength, and areas in which the UK overrelies on foreign suppliers. The Government should then put forward clear long-term investment plans, supported by the National Wealth Fund, to encourage domestic production of priority capabilities.

126. **RECOMMENDATION**
We recommend that Government consult on the changes that may be required to the framework for managing public money in the face of challenges to economic and national security. This should include consideration of whether the tests underpinning managing public money assessments adequately consider economic security imperatives and the benefits of securing both sovereign capabilities and critical supply chains.

6 Diversify critical supply chains

127. Incidents of large-scale supply chain disruptions have increased significantly in recent years. Academics at both the University of Westminster and Aston University, argued that events such as the Covid-19 pandemic and Russia's full-scale invasion of Ukraine highlight the importance of having "multiple pathways for supplies of energy, food, medical supplies, and tech components".[173] Our visits to both Japan and the United States confirmed the steps both nations are now taking to derisk supply chains, particularly from China. We heard first-hand about how the America First Investment Policy will put the United States at a "distance" from strategic competitors, and the work within Japanese companies to build intelligence of their own supply chains, to diversify and to build the strategic stockpiles.

128. In this chapter we consider methods for improving the UK's understanding of its overall dependencies, and the role Government should then play in derisking or diversifying these supply chains.

Understanding supply chain vulnerabilities

129. Various government bodies have responsibility for providing the private sector with intelligence about supply chain issues, including:

- **The Supply Chain Centre:** Announced in the Industrial Strategy, its purpose will be to analyse the inputs that are key to "unlocking growth" for the eight growth-driving sectors (the "IS-8"), and to then "determine what action may be required" to secure these inputs by, for example, building domestic capacity, diversification, or international partnerships.[174]
- **The Critical Minerals Intelligence Centre:** Led by the British Geological Survey with support from the Department for Business and Trade, its primary function is to provide an evaluation of the criticality of minerals to the UK.

173 Dr Karen Jackson (Reader in Economics at University of Westminster); Dr Oleksandr Shepotylo (Senior Lecturer in Economics at Aston University) (ECO0009)

174 Department for Business and Trade, The UK's Modern Industrial Strategy, 23 June 2025

- **The Global Supply Chain Intelligence Programme:** Set up in 2021, this combines large commercial and government datasets with artificial intelligence to map complex multi-tier supply chains.[175] The Department for Business and Trade leads on this programme,[176] although the Government has yet to say how it will interact with the Supply Chain Centre.

- **The Geopolitical Impact Unit:** This provides Foreign, Commonwealth and Development Office intelligence to industry, and also integrates industry's "understanding of trends and challenges" into the department's approach to policymaking.[177]

130. Given the interconnected nature of contemporary supply chains, this decentralised approach risks missing the potential spillover effects of disruptions. The increase in online sales during the Covid-19 pandemic, for instance, led to a shortage of cardboard packing material. This primarily affected retailers, but it also disrupted the supply of batteries used in UK defence equipment.[178] ADS Group called for the Government to "take the lead in consolidating work undertaken in recent years to provide a single version of 'truth' regarding the UK's supply chain vulnerabilities".[179] Academics from the University of Westminster and Aston University told us that the UK "should map its dependencies…to ensure that no critical supply rests on a single point of failure".[180]

131. The Government's Supply Chain Centre will focus on inputs (such as steel or critical minerals) for the eight key growth-driving sectors identified in the Industrial Strategy.[181] It is therefore unclear whether it will play a role in mapping, and mitigating, potential dependencies for UK industry as a whole. By comparison, the European Commission has initiated regular economic security risk assessments, identifying vulnerabilities across key sectors to inform co-ordinated responses at both EU and member state level. These risk assessments have so far focussed on four critical technology areas that were deemed to present immediate risk.[182]

---

175 Altana (ECO0011)

176 Altana, Altana Chosen to Power UK Government's Global Supply Chain Intelligence Programme, 11 June 2025

177 Foreign, Commonwealth & Development Office, The FCDO means business: Foreign Secretary's British Chambers of Commerce speech, 20 March 2025

178 Ministry of Defence, Defence Supply Chain Strategy, 15 November 2022

179 ADS Group (ECO0002)

180 Dr Karen Jackson (Reader in Economics at University of Westminster); Dr Oleksandr Shepotylo (Senior Lecturer in Economics at Aston University) (ECO0009)

181 These are: Advanced Manufacturing, Clean Energy Industries, Creative Industries, Defence, Digital and Technologies, Financial Services, Life Sciences, and Professional and Business Services.

182 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0036)

132. **CONCLUSION**
An understanding of supply chains is critical to a "whole-of-society" approach to economic security. While the new Supply Chain Centre will analyse key inputs, it will do so only in the specific context of the eight growth-driving sectors in the Industrial Strategy. We are concerned that this will only add to the current muddled picture, with new siloed understandings of sectoral vulnerabilities but no overall understanding of the UK's dependencies. The Government cannot take a strategic approach to sovereign capabilities without a clear understanding of the supply chains that support them.

133. **RECOMMENDATION**
The Government should conduct a regular prioritisation exercise with industry and Parliament to identify the UK's critical supply chains. This assessment should combine data regarding critical raw material needs, and possible supply chain disruptions or dependencies, across the economy. From this, the Government should identify which supply chains require strengthening to build the UK's economic resilience. The results from the first of these exercises should be presented to Parliament within the next two years.

Tools to intervene in critical supply chains

134. Once a single centralised understanding of the risks has been established, evidence said that the Government needs to take a more active approach in securing alternative supplies. Helen Kennett told us that this needs a "closer working relationship between Government and industry". For instance, if the intelligence identifies a need to "diversify away" from a certain source, she argued that the Government needs to formulate a "short, medium and long term strategy" that provides the required resilience or alternate sourcing: "Otherwise a lever is pulled, but without there actually being any alternative place for a company to go."[183]

135. Other jurisdictions have taken a more interventionist approach to supply chain resilience, in particular to safeguarding critical minerals. These initiatives have involved the development of stockpiles, partnerships with resource producing states, and measures designed to encourage domestic production. The US Defence Logistics Agency, for example, is seeking to procure up to $1 billion of critical minerals for its stockpiles.[184] Alongside

183 Q32
184 "Pentagon steps up stockpiling of critical minerals with $1bn buying spree", Financial Times, 12 October 2025

this, President Trump's administration is taking various steps to encourage supply chain diversification, such as financing overseas mines,[185] the direct purchase of stakes in projects,[186] and accelerating domestic production.[187]

136. The EU's Critical Raw Materials Act sets out specific benchmarks for the domestic production, processing and recycling of critical minerals.[188] According to RUSI, a "key element" of the EU approach is the designation of 47 strategic projects representing around €22.5 billion in investment.[189] These projects benefit from streamlined planning processes and support in accessing finance. It has also concluded 14 strategic partnerships on raw materials. These non-binding agreements aim to link the EU's industries with resource producing states.[190]

137. Stakeholders from the UK critical minerals sector told us that the Government should focus on removing the barriers to their growth.[191] This would involve simplifying planning procedures, reducing energy costs, and introducing domestic production targets.[192] Mike King, Vice President, Business Development and Government Relations at Cornish Lithium, told us that specific targets would then encourage private investment, by giving "investors the confidence that it was going to be well supported and perhaps incentivised".[193] The Government has said that a new critical minerals strategy will be published before the end of 2025, but it is unclear whether this will adopt a targeted approach for the domestic supply chain.[194]

138. Paul Atherley, Chairman of Pensana, a UK-based rare earth company, also called for the Government to target its support at areas that benefit from a so-called "cluster effect".[195] He highlighted the example of Tees Valley which has access to renewable energy, deep port access, and proximity to its customers: "you set up there, we have people to buy some of our products and we have people who do battery energy storage right next door—we have all the skills available to us".[196] The UK critical minerals midstream and

185 Export-Import Bank of the United States, What is EXIM's Supply Chain Resiliency Initiative?, 15 May 2025
186 "Trump administration pivots to buying stakes in critical sectors", Reuters, 7 October 2025
187 The White House, Executive Order 14241 (Immediate Measures to Increase American Mineral Production), 20 March 2025
188 European Commission, Critical Raw Materials Act (accessed 15 October 2025)
189 The Centre for Finance and Security at the Royal United Services Institute (ECO0036)
190 European Commission, Raw materials diplomacy (accessed 29 October 2025)
191 Q104
192 Q111
193 Q103
194 Minerals PQ 72562, 17 September 2025
195 Q104
196 See previous reference

recycling capability report, produced for the Department for Business and Trade by Frazer Nash Consultancy, similarly called for greater collaboration "between the critical minerals industry and existing regional developments [which] provide commercial opportunities to the critical minerals industry." It highlighted Tees Valley, South Wales and the Southwest as areas that could benefit from closer local collaboration.[197]

139. Our trade agreements can also buttress supply chain security. The upgraded Free Trade Agreement with the Republic of Korea is a potential model for this. The UK Government has said that negotiations have made progress toward "agreeing new supply chains commitments", with the intent to develop "mechanisms that facilitate Government-to-Government dialogue during supply chain disruptions".[198]

140. **CONCLUSION**

The Government's attempts to diversify supply chains, and to safeguard sources of critical minerals, will not be successful unless there is a long-term plan for the UK's supply chain. The forthcoming Critical Minerals Strategy is an opportunity to accelerate this work, and to set out clear priorities. The Government must however go further, and as a matter of policy pursue an alliance of free-trading democracies - such as Canada, which has considerable rare-earth assets - prepared to collaborate in securing mutual supply chains and critical mineral supplies and countering coercive economic behaviour.

141. **RECOMMENDATION**

We recommend that the Government's forthcoming Critical Minerals Strategy:

- Sets specific targets for domestic production, recycling and processing.
- Clearly sets out the UK's approach to diversifying these supply chains through bilateral agreements with allies.
- Designates 'Critical Mineral Clusters' which would benefit from streamlined planning processes and support in accessing finance.

This should be accompanied by clear investment plans for both developing strategic stockpiles and diversifying these supply chains, co-financed by the National Wealth Fund.

197 Frazer-Nash Consulting, UK critical minerals midstream and recycling capability report (PDF), 2 April 2025, p13

198 Republic of Korea: Upgraded Free Trade Agreement, HCWS582, 8 April 2025

7 Defend critical infrastructure, assets and sectors

142. UK industry is being directly targeted by hostile state and non-state actors, threatening the economic security of the country. As a consequence, the cost of implementing security measures has increased significantly for businesses of all sizes in recent years.[199]

Strengthening the UK's approach to cyber security

143. This inquiry has coincided with a spate of high-profile attacks on critical sectors of the UK economy. In April 2025, Co-op and M&S disclosed that they had both suffered significant cyber-attacks, leading to profit losses of £80 million and £300 million respectively.[200] In his evidence, Archie Norman, Chairman of M&S, described the "traumatic" effect the April 2025 cyber-attack had had on staff.[201] Representatives of the Co-op Group told us about staff in their funeral care business having to revert to "paper-based systems" in order to ensure that funerals were not disrupted.[202]

144. Jaguar Land Rover (JLR) was then subject to an attack in August 2025, generating significant operational and financial strain on many suppliers in its supply chain.[203] The Government subsequently provided JLR with a guarantee for a £1.5 billion loan. It is anticipated that this will be used to support JLR's supply chain.[204] These events have highlighted not just the disruptive impact, but also the potential public costs, of increasingly

199 Q129
200 "M&S cyber-attack disruption to last until July", BBC News, 21 May 2025; Co-op Group, Co-op's Underlying Strength Allows The Group To Navigate External Pressures, 25 September 2025
201 Q164
202 Q199
203 "Jaguar Land Rover production severely hit by cyber-attack", BBC News, 2 September 2025
204 Department for Business and Trade, Government back Jaguar Land Rover with £1.5 billion loan guarantee, 28 September 2025

frequent cyber-attacks. Given this, it is essential the UK gets its approach right. From the evidence, we have identified three measures that would strengthen cyber resilience in the UK: introducing liability for software developers, incentivising business investment in cyber resilience, and mandatory reporting following a malicious cyber incident.

145. **CONCLUSION**
Economic security cannot be achieved without cyber security. The spate of cyber-attacks in 2025 has underlined their potential to devastate not just targeted companies, but consumers and wider supply chains. We welcome the steps being taken to build the UK's cyber resilience, but these efforts need to be redoubled in light of recent events.

Liability for software developers

146. The National Cyber Security Centre (NCSC) advocates a 'secure by design' approach to software development, whereby cyber-security is prioritised throughout "all stages of the development life cycle".[205] There is currently, however, no penalty for providers that do not adhere to this approach. Despite the significant public costs if a major cyber-attack occurs, software providers are not liable if an incident is caused by vulnerabilities in their products.[206]

147. So far, the Government's approach to this problem focuses on voluntary standards for software providers. In May 2025, the Government published a Software Security Code of Practice. Katharina Sommer, Group Head of Government Affairs and Analyst Relations at the cyber security firm NCC Group, told us that this aims to incentivise "software developers and procurers of software to pay attention to secure-by-design features in their software".[207] Although it is a voluntary code, and self-assessment is currently the only method for monitoring compliance amongst participants, the Government is working to create a certification scheme based on this compliance process.[208]

148. Other jurisdictions have gone further. The European Union's Cyber Resilience Act, for instance, entered into force in December 2024, and its main obligations will apply from December 2027.[209] Professor Ciaran Martin, former CEO of the NCSC, described this as essentially being a "transfer-of-liability Act, so if the big American tech providers sell faulty products

205 National Cyber Security Centre, NCSC Annual Review 2024, 3 December 2024
206 Q221
207 Q222
208 Department for Science, Innovation & Technology, Software Security Code of Practice, 7 May 2025
209 European Commission, Cyber Resilience Act, 6 March 2025

into the European market, they will be held liable for them".[210] The Act will require manufacturers to factor cyber security into the design and development of their products. Authorities will be able to order the recall of non-compliant products and fine companies that do not adhere to the rules.[211]

149. **CONCLUSION**
The Government's Software Security Code of Practice is a useful first step in encouraging the take up of "secure by design" principles amongst software providers. Compliance with these principles, however, should be the minimum standard rather than a voluntary extra. More needs to be done to ensure that companies are not able to sell software that does not meet cybersecurity standards without being held to account for the damage it may then cause.

150. **RECOMMENDATION**
We recommend that the Government introduce legislation that would mandate the standards set out in its Software Security Code of Practice. Enforcement agencies should be empowered to monitor compliance, and levy penalties against firms that do not adhere to these rules.

The cost of cybersecurity software

151. Richard Horne, CEO of the NCSC, told us that tackling this threat will require a "big funding leap" on cyber security across Government and private sector organisations.[212] In many cases, however, businesses are required to pay extra for software and hardware safety features. According to the NCSC, "unfortunately, many cyber security features (such as multi-factor authentication) are deemed 'premium add-ons'; functionality that involves additional cost for organisations".[213] This can generate difficult trade-offs between security and cost considerations.

152. A further challenge is that much of this expenditure is ineligible for tax relief. Capital allowances are a type of tax relief that enable businesses to deduct some or all of the value of an item from their profits before they pay tax. In many cases new software is paid for through regular payments, akin to a rental, for subscriptions to services based in the cloud. Payments of this kind are classified as revenue, and are therefore not deductible. Archie

210 Q222
211 European Commission, Cyber Resilience Act - Questions and Answers, 1 December 2023
212 Q246
213 National Cyber Security Centre, NCSC Annual Review 2024, 3 December 2024

Norman, Chairman of M&S, told us that these purchases then have to be "expensed in-year. It eats your P and L [profit and loss] as you spend the money".[214]

153. **CONCLUSION**
The cost of cyber resilience has increased significantly in recent years. Key upgrades to software and other IT services are often now made via payments to subscription services rather than one-off purchases, meaning that they are categorised as revenue rather than more tax-efficient capital expenditure. Improved cyber resilience is therefore having a bigger impact on company bottom lines. Businesses should not be forced to choose between resilience and profitability. Government must do more to incentivise investments in cyber security.

154. **RECOMMENDATION**
The Government should amend the capital allowances regime to allow businesses to claim tax relief on subscription-based IT services that directly enhance operational resilience, such as cybersecurity software, legacy system upgrades, business continuity platforms and data protection solutions. A consultation on how this could best be achieved should be launched before the end of the year.

Mandatory reporting

155. Alongside improved cybersecurity systems, we were told that the UK Government lacks an accurate understanding of the scale of cyber-attacks on the private sector. Currently, there is no requirement for a firm to report to the NCSC that it has been the subject of malicious cyber activity. Archie Norman told us that he had reason to believe that there had been "two major cyber-attacks of large British companies in the last four months, which haven't gone reported".[215] Rob Elsey, Group Chief Digital Information Officer at the Co-op Group, said that a central understanding of the threat would be a "great source of information for everyone", helping law enforcement agencies and improving private sector awareness of the threats to their organisations.[216]

156. Archie Norman called for the Government to establish a system that would require companies to inform the National Cyber Security Centre following any "material attack", with 'material' defined in accordance with its scale and the size of the company.[217] Jamie MacColl, Senior Research Fellow in the

214 Q191
215 Q187
216 Q210
217 Q187

Cyber and Tech Research Group at RUSI, agreed and told us that he saw no reason why mandatory reporting should not apply to "all malicious cyber-security incidents".[218]

157. The Government has consulted on proposals to introduce a statutory mandatory reporting regime for ransomware incidents. Its response was published in September 2025. Respondents broadly agreed that a new regime should be introduced, but no timeline has been provided for next steps.[219]

158. **CONCLUSION**
The UK Government will not be able to confront the threat posed by cyber-attacks without an accurate understanding of the scale of the problem. Currently large British companies are not required to report cyber-attacks. This is detrimental to national economic security. A full picture of these incidents is essential to not only the Government, but also to industry, helping both to better understand evolving threats and mitigations.

159. **RECOMMENDATION**
We recommend that the Government consult on proposals for a mandatory malicious cyber incident reporting regime.

Supporting resilience among businesses

The role of insurance

160. Insurance is a key tool in helping businesses manage the impact of systemic risk. When risks have been considered too significant or too uncertain for the market to provide adequate insurance cover, the Government has previously 're-insured' the risks taken on by private insurers. Pool Re, for example, is the longest-established Government-guaranteed reinsurance scheme, and was established to stabilise the market for terrorism insurance for private properties, following the IRA bombings in the early 1990s.[220]

218 Q233
219 Home Office, Government response to ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting, 2 September 2025
220 Pool Re, What We Do (accessed 31 October 2025). Another significant example of Government guaranteed insurance is Flood Re, established following major UK flooding in 2012, after which some homes became uninsurable. Flood Re, What is Flood Re? (accessed 31 October 2025)

161. As cyber threats grow, we have listened carefully to the calls made for further Government intervention in the insurance market. The Joint Committee on the National Security Strategy, in its December 2023 report on ransomware, observed that the UK cyber insurance market is "in an extremely poor state", and concluded that "there is a strong economic case for the Government to do more" on cyber insurance. It recommended that the Government work with the insurance sector to establish a reinsurance scheme for major cyber-attacks.[221] The then Government's response in February 2024 said that its "current, primary focus is to support the insurance industry to strengthen and grow the commercial cyber insurance market".[222]

162. The rise of state-backed cyberattacks has created significant challenges for the insurance industry. Pool Re only covers attacks certified as terrorism by HM Treasury,[223] yet the line between terrorism and hostile state activity is now very blurred. As the 2025 National Security Strategy notes, state actors may "make use of terrorist and criminal groups as their proxies."[224] The losses arising from these incidents may be catastrophic, and in recent years some insurers have updated their policies so as to explicitly exclude government-led cyber-attacks with war-like effects.[225] Despite this, the Government has said that it has no plans to expand Pool Re's remit to cover additional cyber risks.[226]

163. Pool Re's Chief Executive Officer, Tom Clementi, told us that the scope of its cover has expanded since its inception as the terrorism threat has evolved, but that a number of protection gaps still exist which he said "may merit further consideration in the context of the contemporary threat landscape". These include undersea power cables, offshore wind farms, ferries, offshore oil and gas assets, nuclear power stations, residential property and cyber terrorism. Mr Clementi also noted resilience mechanisms can ensure that "when incidents do occur, they are less prolonged and less pronounced

221 Joint Committee on the National Security Strategy, A hostage to fortune: ransomware and UK national security, HC 194, 13 December 2023, paras 68–72

222 Joint Committee on the National Security Strategy, A hostage to fortune: ransomware and UK national security: Government Response, HC 601, 11 March 2024, para 24

223 HM Treasury, Letter from HM Treasury to Pool Reinsurance Limited, 20 August 2025

224 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025

225 Lloyd's of London defines this as an attack that would "(a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state." Lloyd's of London, Market Bulletin: State backed cyber-attack exclusions (PDF), 16 August 2022. See also, Munich RE, War exclusions on the cyber market - Taking the next step, 20 April 2023

226 Pool Re: Cybercrime PQ 78850, 10 October 2025

than would otherwise be the case". He emphasised, however, that Pool Re's status as an arm's-length body of HM Treasury means that matters of policy are ultimately for Government to determine.[227]

164. **CONCLUSION**
With greater and greater private ownership of public risk, there has never been a greater public interest in ensuring that private firms are able to prepare for disruption and recover quickly when it occurs. Risk is inevitable in private enterprise, and the public purse should not be substituted for an effective market. However, the increasingly complicated threat landscape means that the time is now ripe for Government to look again at the insurance market to ensure that it is functioning adequately.

165. **RECOMMENDATION**
The Government should urgently consider expanding the scope of reinsurance schemes such as Pool Re to support private markets which enhance business resilience, particularly in respect of cyber threats.

Funding for SMEs in the supply chain

166. It is important that any increase in the security measures expected from private sector organisations recognises the differing capabilities of businesses. Professor Ciaran Martin told us that it would not be fair to make the same expectations of small businesses as governments or large corporations.[228] Henrik Pederson of Associated British Ports warned that excessive mandatory requirements could make companies uncompetitive.[229]

167. Evidence indicates that SMEs may not have access to adequate capital to make the necessary investments in resilience and security. ADS CEO Kevin Craven told us that: "SMEs struggle day to day with doing business at the moment, and therefore some of these threats are perhaps less of a priority for them".[230] RUSI likewise said that smaller firms would "struggle to implement enhanced cybersecurity measures, investment screening processes, and supply chain diversification".[231]

227 Letter from Pool Re to the Chair relating to potential measures to bolster the UK's economic resilience (PDF), 22 July 2025
228 Q228
229 Q130
230 Q127
231 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0012)

168. This generates risk not only for smaller companies, but for the supply chains of all organisations. In the words of Helen Kennett: "often the focus is on the larger companies, but a company is only as strong as its supply chain".[232] Possible vulnerabilities may serve as a more straightforward target for hostile actors seeking to disrupt critical sectors.

169. Much of the Government's action to improve SME resilience has focussed on either making more guidance available or improving the accessibility of this guidance for small businesses, through the Business Growth Service.[233] The Government announcement of funded Secure Innovation Reviews - a security health check carried out by professionals - for SMEs may be a step in the right direction.[234] However, it was not accompanied by an announcement of grants to implement the findings of these reviews.

170. **CONCLUSION**

A whole-of-society approach means recognising that firms are only as secure as the weakest link in their supply chain. A small company can play an economically critical role. SMEs require more support in their efforts to confront an ever more volatile and uncertain international environment. This support needs to go beyond new guidance and ensure that smaller firms have access to the necessary funding to implement security measures that improve both their resilience and security and that of the national economy.

171. **RECOMMENDATION**

The Government should establish a dedicated SME Resilience Fund, administered by the Department for Business and Trade, to target support at enhancing the cyber resilience of smaller businesses. This fund should integrate with the Government's new Secure Innovation Reviews, by supporting businesses with the money required to make the improvements identified.

232 Q26

233 The Business Growth Service website was launched in June 2025, and aims to bring together Government support and advice for small businesses into a new centralised online offer. Q291

234 Department for Science, Innovation and Technology, New backing for small businesses to protect their intellectual property from security threats, 10 July 2025

Investment screening

172. Alongside ensuring that firms are able to individually defend themselves from threats, the UK must be able to mitigate the national security risks that may arise from investment in the UK's strategic industries. As explained in Chapter 2, these risks are only likely to multiply with the growing capital requirements of UK infrastructure over the coming years.

173. The UK's investment screening regime, as set out in the National Security and Investment Act 2021 (NSIA), is designed to safeguard the UK against a small number of deals that may pose a risk to national security, while leaving most transactions unaffected.[235] We were told, however, that the regime currently casts a wide net over investment activity. CityUK, a body that represents the financial and professional services industries, contended that, "of the transactions reviewed, 95.6% were cleared without the need for an in-depth review", suggesting an opportunity to establish a "more proportionate and efficient process".[236] The Government has recognised how elements of the system may be too burdensome for businesses, and introduced various reforms that aim to reduce this.[237]

174. Evidence received called for the Government to go further and consider ways in which the NSIA system could be used to facilitate friendly investment. RAND Europe, a research organisation, said that the Government should consider the ways in which "restrictive instruments could be turned into enabling ones".[238] For example, blocked investments into UK companies "could be turned into opportunities to proactively identify more suitable investors – domestically or among trusted Allies and Partners via system of coordination and information sharing".[239] Similarly, the British Venture Capital Association (BVCA) suggested the creation of a potential fast-track or pre-approval process for certain types of investors. The purpose of this scheme would then be to create a marketplace of accredited investors "to facilitate investment" into strategic sectors.[240]

175. RUSI's comparative analysis suggests that other jurisdictions have begun to implement similar schemes.[241] The US Defense Department, for example, operates the Trusted Capital Marketplace which "connects vetted small and

235 Cabinet Office, Call for Evidence - National Security and Investment Act, 13 November 2023
236 TheCityUK (ECO0028)
237 Update on the National Security and Investment Act 2021, HCWS878, 22 July 2025
238 RAND Europe (ECO0021)
239 See previous reference
240 British Private Equity and Venture Capital Association (BVCA) (ECO0013)
241 The Centre for Finance and Security at the Royal United Services Institute (ECO0036)

medium-sized technology providers with 'trusted' US capital." A pilot, led by the US Department of the Treasury, is also underway to develop a "fast track process" for investors from "ally and partner sources".[242]

176. **CONCLUSION**

The UK economy needs large quantities of trusted investment. With the UK's growing capital requirements, the Government needs to strike the right balance between facilitating the flow of capital and blocking dangerous acquisitions. The Government is right to recognise that components of the UK's investment screening regime have become too burdensome. It should also, however, go further and consider ways in which this tool can be modernised to encourage investment from trusted sources into critical sectors of the UK economy.

177. **RECOMMENDATION**

We recommend that Government develop an accreditation scheme for providers of trusted capital, similar to the models used in the United States. Accredited investors should benefit from faster turnaround times within the UK's investment screening process, as well as continuous access to dedicated case management at all stages. A marketplace should then be created to connect these investors to companies in critical sectors of the UK economy.

242 US Department of the Treasury, US Department of the Treasury Announces Intent to Launch Fast Track Pilot Program for Foreign Investors, 8 May 2025

8 Deter threats

178. Events such as the full-scale Russian invasion of Ukraine in 2022, and the UK's establishment of an extensive sanctions regime in response, have highlighted the importance of trade and financial measures to the UK's overall defence and security toolkit. The Government now has a variety of tools, set out in Table 5, that can be used to either protect the UK's economic interests or pursue foreign policy objectives.

179. Evidence we received suggests that the effectiveness of these measures is being significantly undermined by a lack of enforcement. In the context of economic crime, Dan Neidle, a tax lawyer and founder of Tax Policy Associates, told us that there needed to be a "step change, not in the regulations and the rules, but in the enforcement"; in his words, "if you have rules and they are not enforced, they may as well not exist".[243] In the remainder of this Chapter, we explore the evidence of the poor enforcement of these regimes, and consider the ways in which the UK toolkit should now evolve to deter new threats.

243 Business and Trade Sub-Committee on Economic Security, Arms and Export Controls, Oral evidence: Economic Crime, HC 798, Wednesday 19 March 2025, Q3

Table 5: Deterring threats to economic security: toolkit

Regime	What are they?	Statutory framework	Management and enforcement
Trade sanctions	Restrictions on the export, import, or movement of specific goods, technology and services often relating to a particular country. They may be imposed for a broad range of purposes, including national security or foreign policy objectives.	Sanctions and Anti-Money Laundering Act 2018	Criminal enforcement of trade sanctions is the responsibility of HM Revenue and Customs (HMRC). Civil enforcement and co-ordination of trade sanctions is supported by the Office for Trade Sanctions Implementation in the Department for Business and Trade.[244]
Export controls	Government controls on the export of a range of both military and 'dual-use' goods.	Export Control Act 2002 Export Control Order 2008	Management of UK strategic export controls sits under the Department for Business and Trade via the Export Control Joint Unit (ECJU), which coordinates its work with other relevant departments, such as the Ministry of Defence. Enforcement is the responsibility of HM Revenue and Customs.[245]

244 Department for Business and Trade and Export Control Joint Unit, Trade sanctions, arms embargoes, and other trade restrictions (accessed 11 November 2025); Department for Business and Trade and Office of Trade Sanctions Implementation, Trade sanctions: civil enforcement (accessed 11 November 2025)

245 Export Control Joint Unit, Department for International Trade and Department for Business and Trade, UK strategic export controls (accessed 11 November 2025); Export Control Joint Unit and Department for Business and Trade, UK strategic export controls annual report 2024, 18 July 2025

Regime	What are they?	Statutory framework	Management and enforcement
Deterring economic crime	Economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others.	There are various pieces of relevant legislation including the Criminal Finances Act 2017, the Bribery Act 2010, and most recently, the Economic Crime and Corporate Transparency Act 2023.	The UK's response is co-ordinated through the National Economic Crime Centre, housed in the National Crime Agency under the oversight of the Minister of State for Security. Agencies such as the Serious Fraud Office and the National Crime Agency investigate economic crimes such as fraud or money laundering. The 2023 Act also granted new powers to Companies House, enabling and requiring it to undertake a policy of proactive enforcement.[246]

246 Home Office et al, Economic Crime and Corporate Transparency Act: economic crime in the UK, (accessed 11 November 2025); National Crime Agency, National Economic Crime Centre (accessed 11 November 2025); GOV.UK, Minister of State (Minister for Security) (accessed 11 November 2025); Economic Crime and Corporate Transparency Act 2023

Regime	What are they?	Statutory framework	Management and enforcement
Trade remedies	Measures put in place to help protect UK businesses from unfair trade practices, such as dumping. Typically, this takes the form of additional tariffs and/or quotas on imports.	Taxation (Cross-border Trade) Act 2018 Trade Act 2021	The Trade Remedies Authority, an executive non-departmental public body, sponsored by the Department for Business and Trade, is responsible for investigating unfair practices and making recommendations. The Secretary of State for Business and Trade then takes the final decision on whether to accept or reject these recommendations.[247]

Export controls and sanctions breaches

180. Parliamentary committees have long expressed concern about the lack of prosecutions for breaches of strategic export controls or sanctions. In 2022, the Committees on Arms Export Controls found that from 2007–2021, there were only 26 HMRC strategic exports and sanctions prosecutions.[248]

181. Another long-standing call for improvement is the transparency available in respect of compound settlements. A compound settlement is a penalty offered, and agreed with the company or entity, for breaches of export controls or sanctions in lieu of criminal prosecution. These penalties can be significant. For instance, the ECJU announced a settlement of £1,160,725.67 in July 2025. This was the largest compound settlement HMRC had concluded for a Russia sanctions offence.[249] The ECJU publishes the dates and amounts of such settlements, but it is HMRC policy to not publish the

247 Trade Remedies Authority, Introduction to trade remedies (accessed 11 November 2025); Trade Remedies Authority, Annual Report and Accounts 2024–25 (PDF), 17 July 2025, p. 6

248 Committees on Arms Export Controls, Developments in UK Strategic Export Controls, HC282, 28 October 2022, para 70

249 HMRC and ECJU, NTE 2025/18: compound settlement for breaches of export control, 8 July 2025

details of the items exported, or the companies accepting the settlement. In 2022, HMRC justified this on the basis that disclosure would not "drive compliance, promote voluntary disclosure or be proportionate".[250]

182. The Committees on Arms Export Controls, while recognising that there may be issues with public disclosure, concluded that it saw no reason why this information could not be provided privately to allow for "effective scrutiny".[251] The previous Government rejected this recommendation on the basis that disclosure protocols were a matter for HMRC, and they had already set out their position that this would not be in the public interest.[252] This is different to the approach taken in other parts of the toolkit. The Office for Financial Sanctions Implementation, for instance, publishes the equivalent information for breaches of financial sanctions.[253]

183. **CONCLUSION**

Economy security requires not just resilience at home, but also effective deterrence of future threats. Improving the deterrent effect of trade sanctions and export controls requires greater transparency in enforcement outcomes. Breaches of either sanctions or export controls, even when resulting from error, are a serious matter, and businesses should not always be able to avoid the reputational harm of being publicly identified when they commit a breach. This is already recognised in the context of financial sanctions, where disclosure of breaches is already commonplace.

184. **RECOMMENDATION**

Building on the 2022 recommendation of the Committees on Arms Export Controls, we ask the Government to clarify if there are any situations whatsoever in which it believes disclosure of the names of companies or individuals that enter into compound settlements for breaches of trade sanctions and strategic export controls would be lawful and in the public interest. Where such barriers may exist to limit disclosure, these should be removed.

250 Committees on Arms Export Controls, Developments in UK Strategic Export Controls, HC282, 28 October 2022, para 72

251 See previous reference, para 76

252 Ministry of Defence, Department for International Trade, and the Foreign, Commonwealth & Development Office, First Joint Report of the Committees on Arms Export Controls Session 2022–23 Developments in UK Strategic Export Controls: Response of the Secretaries of State for International Trade, Defence, Foreign, Commonwealth and Development Affairs (PDF), CP 775, January 2023, p10

253 Office for Financial Sanctions Implementation and HM Treasury, Financial sanctions enforcement: decisions and monetary penalties imposed, 30 September 2025

Corporate fraud

185. As set out in Chapter 2, we heard significant evidence of the abuse of the Companies House register to facilitate money laundering, sanctions evasion, and corporate fraud. Despite this, Dan Neidle told us that there had been no prosecutions for breaches of the rules requiring companies to identify the person who owns or controls it in 2022, and four in the first quarter of 2023.[254] Companies House can also issue fines to company directors who fail to file company accounts on time. In 2023–24, Companies House issued £158 million in fines, but only collected £73.5 million, just 46%. In 2019–20, Companies House collected 57%.[255]

186. The Economic Crime and Corporate Transparency Act 2023 gave Companies House new powers to prosecute directors for non-compliance of certain obligations under the Companies Act 2006. Louise Smyth, then CEO and Registrar at Companies House, told us in March 2025 that they had yet to use these powers, but the "next thing that we need to get on to is prosecutions".[256] Its business plan for 2025–26 includes an objective to "use our new powers to enforce our registrars' objectives by taking action in relation to 150,000 companies".[257] Progress against this metric is difficult to measure, as Companies House currently only publishes an annual summary of its total civil penalties and prosecutions, with no detail provided on individual cases.

187. **CONCLUSION**
Abuse of company registration has the potential to undermine the UK's deterrence regime. Companies House's new powers have the potential to make a significant difference in the fight against economic crime. In order to be effective, its implementation of these powers must focus on a significant improvement in the frequency of enforcement action.

188. **RECOMMENDATION**
We recommend that Companies House steps up its disclosure of successful enforcement activity. The names of individuals who have been successfully prosecuted should be disclosed immediately following conviction, to both name and shame those involved in wrongdoing, and to highlight Companies House's progress in improving its approach to enforcement.

254 Business and Trade Sub-Committee on Economic Security, Arms and Export Controls, Oral evidence: Economic Crime, HC 798, Wednesday 19 March 2025, Q4

255 "UK companies pay less than half of fines issued for filing accounts late", Financial Times, 23 February 2025

256 Business and Trade Sub-Committee on Economic Security, Arms and Export Controls, Oral evidence: Economic Crime, HC 798, Wednesday 19 March 2025, Q58

257 Companies House, Companies House business plan 2025 to 2026, 17 June 2025

Resourcing and staffing

189. Evidence suggests that a lack of resources for enforcement agencies helps explain poor enforcement. In February 2024, Kathryn Westmore, a Senior Research Fellow at RUSI, told our predecessor Committee that the amount being invested in Companies House was not "commensurate to the risk that the abuse of Companies House has posed". She contended that it would require "five, if not more, times" the investment for Companies House to put the necessary controls in place.[258]

190. When we raised resourcing issues with these organisations, they highlighted difficulties in recruiting staff as a significant barrier to improving enforcement. In March 2025, Companies House told us that they had a 15% overall vacancy rate, rising to 20% for digital roles.[259] They highlighted disparities between their pay scale and Government Departments as a particular concern: "We have people who leave us to go to a job at the same grade in another Department that is £15,000 more, and we can't even compete with that".[260]

191. Similarly, James Babbage, Director General for Threats at the National Crime Agency (NCA), told us that the salaries his organisation could offer were "not particularly competitive compared with policing or the UK intelligence community, and still less competitive against industry".[261] The NCA is a non-ministerial government department, rather than a police force, and as such is subject to different pay parameters than policing. In 2024, the median pay gap between the NCA's Grade 1 pay band and the equivalent rank in the police force was £29,680.[262]

192. **CONCLUSION**

The UK's ability to deter economic threats depends upon agencies having the necessary staff in place to investigate wrongdoing. Currently, the UK depends on professionals committed to keeping the country safe, but today's pay scales mean that frontline enforcement agencies cannot attract the staff they need to adequately police the threat. Disparities with the private sector are significant - but so are disparities with the salaries of other public servants in similar ranks.

258 Business and Trade Committee, Oral evidence: Implementation of Economic Crime and Corporate Transparency Act 2023, HC 522 Tuesday 6 February 2024, Qq113–115

259 Business and Trade Sub-Committee on Economic Security, Arms and Export Controls, Oral evidence: Economic Crime, HC 798, Wednesday 19 March 2025, Qq26–27

260 Business and Trade Sub-Committee on Economic Security, Arms and Export Controls, Oral evidence: Economic Crime, HC 798, Wednesday 19 March 2025, Q46

261 Q247

262 Letter from the National Crime Agency to the Chair relating to pay differentials between NCA Officers and Police Officers (PDF), 21 July 2025

193. **RECOMMENDATION**
We recommend that the Government urgently considers changing pay scales at organisations such as the National Crime Agency and Companies House, to ensure that salaries of mission critical staff keep pace with industry and fully reflect the indispensable work they do.

Anti-coercion measures

194. The UK must not only improve enforcement of the current deterrence toolkit, but consider new tools for deterring novel economic threats.[263] The 2025 National Security Strategy argues that, as the rules governing the international trading system break down, more states will seek to "weaponise trade or use export controls and supply chain dependencies to gain advantage".[264] In response, according to Chatham House, other countries have already begun to develop "sophisticated retaliatory toolkits, countermeasures, and coercive restrictions designed to both coerce and deter/respond to coercion".[265]

195. The Government has recognised that the current trade remedies system does not adequately guard against threats such as the "strategic weaponisation of trade".[266] It has committed, when Parliamentary time allows, to expanding the Trade Remedies Authority's powers to respond to unfair trading practices and consulting on new powers to respond to economic coercion.

196. Submitters, however, writing before the Trade Strategy's publication, expressed scepticism as to the efficacy of the current UK system, especially in comparison to the tools available to other states. The Centre for Economic Security, a research organisation, told us that there is currently "no…established mechanism in the UK comparable to the EU's anti-coercion measures or 'the firm' by the US", referring to the US' Countering Economic Coercion Act 2023.[267]

197. The European Union's Anti-Coercion Instrument, which came into force in December 2023, sets out a framework that aims to protect member states from coercive practices. Chatham House said that this involves a defined "decision-making and consultation process", an emphasis on negotiation, and a wide array of retaliatory options if a solution cannot be reached,

263 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0012); Dr Karen Jackson (Reader in Economics at University of Westminster); Dr Oleksandr Shepotylo (Senior Lecturer in Economics at Aston University) (ECO0009)
264 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025
265 Chatham House (ECO0018)
266 Department for Business and Trade, The UK's Trade Strategy, 26 June 2025
267 Centre for Economic Security (ECO0003)

including "restrictions on trade (goods and/or services), investment, procurement, and access to EU programmes".[268] Under the UK's system, trade remedies can only apply to goods and typically take the form of additional tariffs or quotas on imports.

198. **CONCLUSION**
In today's volatile geopolitical climate, the UK must be able to defend itself against economic coercion from hostile actors. The Trade Strategy correctly recognises that today's trade remedies system does not adequately protect us against emerging economic threats. As economic coercion becomes more prevalent, the Government must go further and consider whether a new framework is now required to adequately protect the UK from coercive economic practices.

199. **RECOMMENDATION**
The Government should establish a specific Anti-Coercion Instrument, and urgently launch a consultation on its design. Measures proposed should include a formal framework for responding to economic coercion and widening the available countermeasures to include restrictions on services trade, limitations on foreign direct investment and public procurement, and the suspension of intellectual property right protections.

268 Chatham House (ECO0018). For more information on this process see European Parliamentary Research Service, EU anti-coercion instrument (PDF), 2022, p13

9 Dovetail approaches domestically and internationally

200. Threats to economic security do not stop at the UK's borders, nor do our adversaries target us alone. The UK faces direct attacks, but given the interconnectedness of our supply chains and defence and security industries, we are at risk when our allies are attacked too. That is why an essential component of economic security strategy is to dovetail the UK's approach with the work of our partners.

201. This final Chapter sets out how the UK Government should integrate economic security into its bilateral relationships with partners and allies.

Aligning with allies

202. Our visits to the European Union institutions, the WTO, Japan and the United States taught us that economic security is now inseparable from trade and geopolitical dialogue.

203. Our report on strengthening UK-EU relations noted that, while the UK-EU Trade and Cooperation Agreement (TCA) lacks a formal economic security dialogue, there is support among stakeholders for structured UK-EU coordination on issues such as supply chain resilience, competition policy, and global trade governance that helps advance the UK's interests and those of the EU.[269] We recommended that the UK work closely with the EU to strengthen coordinated action against non-market economies that undermine the international trading system through unfair practices.[270] In

269 In June 2023, the European Commission published the EU's first dedicated Economic Security Strategy, with three priorities: promoting EU competitiveness; protecting the EU from identified economic security risks; and partnering with "the broadest possible range of partners to reinforce economic security, foster resilient and sustainable value chains, and strengthen the international rules-based economic order and multilateral institutions". European Commission, Joint communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy", 20 June 2023

270 Business and Trade Committee, How to strengthen UK-EU relations: Policy Priorities for the Summit (PDF), HC 908, 15 May 2025, para 15

response, the Government stated that the UK and EU would "explore ways to exchange views on external aspects of their respective economic security policies, including through formal dialogues".[271]

204. In our report on trade with the Asia-Pacific region, we observed that both the UK and Asia-Pacific countries are exposed to many of the same dependencies on critical supply chains and critical supply chains that emanate from China. It is in the UK's shared interest to strengthen both the UK and Japan's resilience to risks and to diversify sourcing. The tri-national Global Combat Air Programme (GCAP) partnership with Japan and Italy provides a bedrock upon which greater trading ties can be created in defence and other sectors. We recommended that the UK Government explore with Japan the potential to widen the partnership to include digital and cyber technologies, and quickly deepen economic security dialogues with Asia-Pacific allies to enhance mutual resilience and diversity of supply chains.[272] In response, the Government told us that the UK and Japan's Industrial Strategy Partnership includes work to "formalise cooperation across our complementary strengths in frontier industries to build greater economic resilience and growth opportunities". It also noted that the UK Government has existing economic security dialogues with Australia and Japan, with work continuing on matters including supply chain resilience.[273]

205. The UK's relationship with the US has been marked by increasingly explicit recognition of shared economic security priorities in recent years. In June 2023, the two countries agreed the Atlantic Declaration, establishing a framework for 21st-century economic cooperation built around five pillars: technology, economic security, digital transformation, clean energy, and defence collaboration.[274] The General Terms of a UK-US Economic Prosperity Deal, published in May 2025, announced both countries' intention to "strengthen cooperation on economic security, including by coordinating to address non-market policies of third countries", and to "cooperate on the effective use of investment security measures, export controls, and ICT vendor security".[275] In our report on the US Economic Prosperity Deal, we argued that the UK must approach trade negotiations with the United

271 Business and Trade Committee, How to strengthen UK-EU relations: Policy Priorities for the Summit: Government Response (PDF), HC 1267, 5 September 2025, p. 3

272 Business and Trade Committee, Export led growth: Trade with the Asia-Pacific region (PDF), HC 1048, 29 June 2025, paras 29–35

273 Business and Trade Committee, Export led growth: Trade with the Asia-Pacific Region: Government Response (PDF), HC 1324, 19 September 2025, p. 3

274 House of Commons Library, What is a trade deal? UK-US trade talks since 2020 (PDF), CBP 10316, 30 July 2025

275 HM Government, General Terms for the United States of America and the United Kingdom of Great Britain and Northern Ireland Economic Prosperity Deal (PDF), 8 May 2025, p. 4

States as a component of a broader economic and foreign policy strategy focussed on ensuring Western leadership in the face of global competition, particularly from China.[276]

206. In particular, we recommended that any future digital trade negotiations must strike a careful balance between promoting cross-border collaboration to strengthen the Western alliance, safeguarding intellectual property and enabling the development of sovereign UK AI capabilities,[277] though we note that in August 2025, the US partially reversed stricter licensing requirements on Nvidia AI chip exports to China, illustrating the uncertainty facing UK firms reliant on US technology supply chains.[278] In September 2025, the UK and US published a Memorandum of Understanding for a new Technology Prosperity Deal, setting out (among other measures) plans to collaborate closely on AI to "enable adoption and advance our collective security". The MoU also stated that the two countries intend to collaborate on securing and scaling private capital towards the development of "advanced critical technologies".[279]

207. Furthermore, bilateral trade relationships have the potential to reinforce security of supply chains. The UK Government has said that FTA negotiations with the Republic of Korea have made progress toward "agreeing new supply chains commitments", with the intent to develop "mechanisms that facilitate Government-to-Government dialogue during supply chain disruptions".[280] It will be important for the UK to seize the full potential of trade agreements to enhance various aspects of economic security.

208. **CONCLUSION**

Economic security must form a core component of the UK's international trading and geopolitical relationships. We reiterate our recommendations to deepen economic security co-operation with the United States, European Union and Asia-Pacific countries. In particular, a central pillar of the UK's trade strategy must be the establishment and maintenance of Western leadership in the race for technological superiority, particularly against China. Trade negotiations must identify opportunities to reinforce supply chain security through co-operation with allies, by exploring similar mechanisms to those being pursued in negotiations with the Republic of Korea.

276 Business and Trade Committee, US Economic Prosperity Deal (PDF), HC 1306, 14 September 2025, para 106

277 See previous reference, para 116

278 See previous reference, para 122

279 Prime Minister's Office, Memorandum of Understanding between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland regarding the Technology Prosperity Deal, 18 September 2025

280 Republic of Korea: Upgraded Free Trade Agreement, HCWS582, 8 April 2025

209. **CONCLUSION**
We welcome steps to establish economic security dialogues, but encourage these to develop in a more structured way. The ultimate aim of these endeavours should be an alliance of free trading democracies, leveraging bilateral and multilateral trading relationships to secure supply chains and counter coercive activities.

210. **RECOMMENDATION**
The Government should prioritise in trade negotiations measures which will mutually benefit the economic security of the UK and key partners. The UK should proactively identify opportunities to align its economic security approach with those of trading partners. The Government should also commit to ongoing, structured dialogue with the United States, the European Union and Asia-Pacific countries on economic security, including supply chain resilience, investment security and technology leadership.

The role of international institutions

211. Evidence emphasised the importance of working through international multilateral institutions, alongside aligning with allies, despite challenges to the rules-based order. The 2025 National Security Strategy argues that, whilst the national interest is best served by preserving "effective multilateral cooperation on issues from economic stability to energy policy", many of these rules are now being eroded.[281] It contends that, looking forward, there will be less scope for "agreement on mechanisms which protect fair trade, set controls on science and technological developments and mitigate the effects of climate change, as multilateral institutions decline in influence".[282]

212. In response to this, however, submitters called for the UK to more assertively use its influence to rebuild support for these norms. RUSI told us that the UK should "work to strengthen the enforcement of international economic security laws and norms", by leveraging its leadership role in organisations such as the WTO and G20.[283] Likewise, academics from the University of Westminster and Aston University told us that, by working through such institutions, the UK could promote dispute resolution and therefore "help mitigate" current tensions in the global trade environment.[284] Trade

281 Cabinet Office, National Security Strategy 2025: Security for the British People in a Dangerous World, 24 June 2025
282 See previous reference
283 Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) (ECO0012)
284 Dr Karen Jackson (Reader in Economics at University of Westminster); Dr Oleksandr Shepotylo (Senior Lecturer in Economics at Aston University) (ECO0009)

association for the technology sector techUK contended that the UK could "play a key role in convening a coalition of the willing in support of multilateralism and rules-based trade".[285] Multilateral trade agreements also have a role to play, with a key message from our visit to Japan in March/April 2025 being that the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is viewed as much as a geopolitical tool as a trade agreement.

213. **CONCLUSION**
The UK has long benefited from the maintenance of an open international trading system. It must not acquiesce in the erosion of a global trading system that it is in our national interest to defend and to advance. The UK should continue to use its international influence to build support for renewed adherence to these rules.

214. **RECOMMENDATION**
We recommend that the Government approach its engagement with multilateral institutions with a renewed focus on the promotion of the rules-based trading system. It should set out to us in writing, with examples, how it is doing so.

285 techUK (ECO0030)

Conclusion

215. The threats facing the United Kingdom's economic security are large, diffuse and growing. The evidence we have gathered since March 2025 makes clear the essential first steps that the UK must take to address this challenge: the adoption of a new economic security doctrine with clear strategic principles to underpin the UK approach; a holistic approach to threat assessment involving the private sector; the adoption of a coherent institutional framework across Government; and a truly whole-of-society approach, underpinned by strong public-private partnership and accompanied by robust Parliamentary scrutiny. Without these steps, the UK's approach to economic security risks becoming ever more uncoordinated and outpaced in an increasingly multipolar and unstable world.

216. The recommendations set out in this Report are essential, but they are only the necessary first steps in consolidating a new approach to economic security. To ensure the UK's economic security strategy is fit not just for the times in which we live, but for future challenges, much more will need to be done. This Sub-Committee will continue to scrutinise the UK's approach to economic security in the coming years, highlighting new threats as they arise and recommending further improvements to our toolkit. In this way, we are determined to help Parliament play its part in a truly whole-of-society approach.

Annex: Note of visits to the European Union institutions, Japan and the United States

1. The Committee undertook visits to Brussels (in January 2025), Japan (in March/April 2025) and Washington DC (in June 2025) in connection with a number of ongoing inquiries. These visits yielded valuable evidence for our baseline assessment of UK economic security, complementing the comparative analysis undertaken by RUSI and presented in Chapter 3 of this Report. This Annex presents a summary of the key findings from these visits relating to economic security.

2. As well as this inquiry, these visits also informed the development of our reports on How to strengthen UK-EU relations,[286] Trade with the Asia-Pacific region[287] and the US Economic Prosperity Deal.[288] We are grateful to all those, including British Embassy staff in-country, who helped make these visits possible.

European Union

3. The Committee visited Brussels (as well as the World Trade Organisation) in late January 2025, engaging with trade experts, industry representatives, European Parliament colleagues, and HM Government officials to gain insights into the key trade-related issues.

4. Our meetings included discussion of how both the EU and the United States are evolving their approach to economic security, particularly in respect of China. We met with EU officials to discuss the three pillars of the EU Economic Security Strategy (promote, protect and partner), and how the EU is positioning itself in the shifting global trading environment. We also met

286 Business and Trade Committee, How to strengthen UK-EU relations: Policy Priorities for the Summit (PDF), HC 908, 15 May 2025

287 Business and Trade Committee, Export led growth: Trade with the Asia-Pacific region (PDF), HC 1048, 29 June 2025

288 Business and Trade Committee, US Economic Prosperity Deal (PDF), HC 1306, 14 September 2025

with the Mercator Institute for China Studies (MERICS) and discussed their recent country profile on the UK, which found that the UK "excels" in building resilience against China, "except in the economic sphere".[289]

Japan

5. The Committee visited Japan between 30 March and 4 April 2025, to inform our inquiries and to examine the opportunities for bilateral trade.

6. We held discussions with Japan's Ministry of Economy, Trade and Industry (METI), who told us that economic security is central to one of the missions in Japan's industrial strategy launched in 2021. Our discussions in Japan emphasised the importance of public-private partnership to ensure economic security. We heard how Keidanren (the Japan Business Federation) had been part of an expert panel convened to help design Japan's Economic Security Protection Act. Businesses reported that, since the Act was introduced, they are having more frequent conversations with Government on issues such as supply chain resilience. A key focus in the industrial strategy has been on critical enabling technologies, such as batteries and semiconductors, and one firm told us that even in small quantities a failure to access critical minerals would have significant implications.

7. Inside companies themselves, we heard that more are developing their own economic security teams and building up their intelligence capability. There was a broad view that companies now, more so than in the past, need to understand where the pinch points lie in their supply chains. One firm told us that it had conducted a survey using AI to monitor the supply chain for some 180,000 items. There is increasing caution in Japanese companies about dealings with China, and greater consideration of how to mitigate the risks associated with such activities.

8. Relevant to our recommendation of the need to dovetail approaches with allies, we heard that in Japan the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is viewed as much as a geopolitical tool as a trade agreement, and that the UK's accession to the Agreement was welcomed.

289 MERICS, Profiling European countries' resilience towards China, 31 October 2024

United States

9. The Committee visited Washington DC from 9 to 10 June 2025. We met senior figures in the White House, across Congress, the Office of the U.S. Trade Representative (USTR), and key industry stakeholders to understand US trade priorities and next steps for the UK-US Economic Prosperity Deal. Much discussion with business focussed on the then yet to be finalised US-UK technology partnership.

10. Our meeting with USTR emphasised the Administration's view that economic security now needs to be embedded into trade policy, rather than siloed in foreign policy or security policy, and that like-minded trade partners should take action aligned with the US. We also met with the Committee on Foreign Investment in the United States (CFIUS), an interagency committee tasked with reviewing certain transactions involving foreign investment and certain real estate transactions by foreign persons. We heard about the steps being taken under the America First Investment Policy to put the United States at a "distance" from strategic competitors such as China, and a recent series of Executive Orders targeting critical minerals in particular. There was also discussion of the US's interest in derisking not just US supply chains, but also those of the UK, and the value of identifying mutually beneficial investment opportunities.

11. China featured prominently in nearly every meeting we held in Washington. US officials and think tanks expressed deep concern over China's non-market practices and its impact on global trade norms. There is growing support in Washington for a plurilateral approach to counter China's economic model, potentially outside the World Trade Organisation (WTO), with some advocating for a new global trade framework that better reflects current geopolitical realities.

Conclusions and recommendations

Defining economic security

1. Economic security is fundamental to national security. We welcome the Government's recognition of this. By its very nature however, only industry and Government working jointly and severally together can safeguard the UK's economic security through the 'whole of society approach' to defence which the Prime Minister has said the times now require. New safeguards however will not come without cost. On the contrary, a stronger defence of our economic security will require sustained long-term public and private investment. This in turn will require both clarity and certainty about the Government's objectives, well beyond the life of one Parliament. (Conclusion, Paragraph 19)

2. In the face of a fast-changing international environment, a fixed, formal definition of 'economic security' is likely to be unworkable. However, as demonstrated by CONTEST, Government can guide policymakers and businesses by clearly setting out the principles of a long-term approach in a new and clearly articulated economic security doctrine. (Conclusion, Paragraph 20)

3. The Government should adopt, and clearly set out, the strategic principles of a new doctrine for economic security. From our consideration of the evidence and comparisons with other jurisdictions, we recommend that this might best incorporate six core principles - the '6Ds':

    - Diagnose and regularly share an understanding of threats to the UK's economic security.
    - Develop sovereign capabilities in areas critical for UK economic security.
    - Diversify critical supply chains, energy sources and technology inputs to reduce risks of disruption and coercion, through combined action with allies.

- Defend critical and vitally significant infrastructure, other important national assets such as data, intellectual property to prevent technology leakage, and critical sectors through building resilience, especially in cyber space.
- Deter threats to UK economic interests through proactive enforcement of offensive economic measures, such as sanctions, at home and abroad.
- Dovetail public-private co-operation domestically and internationally, aligning and collaborating with allies, and ensuring a concerted and joined-up effort across the nation and the UK's alliances. (Recommendation, paragraph 21)

4. Safeguarding economic security will always involve calculated trade-offs. Principles will often conflict. No government therefore can eliminate all ambiguity for businesses and policymakers. This is where political leadership is crucial. It is for the Government to set out how it has chosen to make trade-offs and to prioritise between different principles in any given situation. In turn, it is for Parliament to scrutinise the choices made by Government, to challenge and ensure democratic legitimacy. (Conclusion, Paragraph 22)

5. To ensure both clarity and long-term certainty for the UK's economic security regime, the Government should consider enshrining the key recommendations in this Report via a new Economic Security Bill. This would allow Parliament to be fully engaged in providing a new, stronger foundation to the UK's economic security. (Recommendation, paragraph 23)

Threat assessment

6. The Government has published a multitude of security reviews and sectoral evaluations, but not a single consolidated assessment of the threats to UK economic security. Given the lack of a "single source of truth", we have decided to summarise our own baseline assessment of economic security threats. We hope that Parliament will enhance and develop this 'parliamentary view' over the years ahead. From our evidence, we have identified ten elements of the threat landscape facing the UK economy:

i. Transnational risks;

ii. Disruption to worldwide market competition;

iii. State threats, including the coercive use of economic tools;

iv. Supply chain disruptions, along with threats to transport and sea lanes;

v. Critical minerals;

vi. Critical National Infrastructure (CNI);

vii. Cyber and emerging technology;

viii. Illicit finance and money laundering;

ix. Foreign investment in critical sectors of the UK economy; and

x. People-focussed threats, such as intellectual property (IP) theft or physical threats to executives. (Conclusion, Paragraph 31)

7. Together these threats point to a transformed threat landscape in which we are likely to see a radical expansion in the private ownership of public risk. This underlines the absolute imperative of rethinking the way state and market work together to safeguard economic security. Most challenging of all is the reality that rarely will any single one of these risks present alone. Instead, they may combine in ways that the UK may struggle to manage. (Conclusion, Paragraph 32)

8. The UK faces increasingly complex transnational threats. The devastating impacts of the Covid-19 pandemic and the rapidly changing climate are two examples of existential challenges, against which the UK economy must become more resilient. (Conclusion, Paragraph 35)

9. The UK faces unprecedented disruption to the international economic order. As many powers prioritise self-interest above adherence to the rules-based system, the UK economy faces new risks of economic damage that may jeopardise the UK's growth objectives. (Conclusion, Paragraph 37)

10. Threats to the UK from state actors that fall short of military action are continuing to grow. Foreign powers are increasingly willing to coerce or undermine others using economic tools or by exploiting economic interdependencies. Russia, China, Iran and North Korea are most often cited as being directly or indirectly responsible for hostile acts targeting the UK. However, actions taken by the UK's allies—as part of intensifying political, economic and technological competition globally—also contribute to geopolitical uncertainty and economic instability. (Conclusion, Paragraph 43)

11. The world has never been more interconnected, and the UK economy is dependent on complex and interwoven supply chains. Consumers, businesses and public institutions rely on supply chains where objects repeatedly cross borders, often on a "just-in-time" basis where the slightest disruption can have enormous impacts. The complexity of supply chains promotes efficiency, low prices and consumer choice, but leaves the UK economy vulnerable. (Conclusion, Paragraph 46)

12. Maritime infrastructure, together with the UK's telecommunications and energy systems, underpin these supply chains. The events of recent years, notably Houthi attacks on commercial ships in the Red Sea, have demonstrated the continuing centrality of maritime security to the UK economy. Increasing global instability means maritime security is more important than ever. (Conclusion, Paragraph 47)

13. Over the coming years, emerging technologies and the net zero transition will increase global demand for critical minerals exponentially. The absence of any significant domestic presence in the mineral value chain leaves the UK significantly exposed to disruptions in their supply. There is considerable potential for adversaries to use this to their advantage, while the UK has no equivalent strategic leverage. (Conclusion, Paragraph 50)

14. The UK's existing critical national infrastructure is vulnerable to a range of threats, from extreme weather to cyber-attacks. In expanding and renewing that infrastructure in response to a growing population and the net zero transition, the UK may be forced to re-evaluate the trade off between on the one hand, lower cost technology and investment from China, and on the other, the risks to resilience that would entail. (Conclusion, Paragraph 53)

15. Cyber threats to the UK's economy, institutions and infrastructure continue to evolve. A string of high-profile attacks in 2025 have vividly demonstrated the devastating impacts of these attacks on workers, consumers and associated supply chains. The boundary between "state" and "non-state" cyber-attackers is becoming increasingly blurred, and the rapid emergence of new technologies will exponentially multiply the damage they can inflict. (Conclusion, Paragraph 56)

16. The UK's long-standing status as a global financial centre is both a crucial economic strength, and a potential vulnerability that must not be overlooked. Inadequate safeguards against sanctions evasion and money laundering risk undermining the effectiveness of the UK's economic security toolkit. (Conclusion, Paragraph 58)

17. The UK's reliance on foreign direct investment risks a loss of control over emerging companies in industries critical to the national interest. Capabilities developed by the UK defence and emerging technology sectors are increasingly being targeted by foreign firms and governments. (Conclusion, Paragraph 60)

18. In increasing the resilience of institutions and technology, the UK must not lose sight of people-based threats. People are an organisation's greatest asset, but they can also be its most unpredictable vulnerability. The UK's adversaries can be expected to target individuals for influence, blackmail,

espionage and even physical harm. As more sectors of the economy are recognised for their importance to economic security, so must the UK's appreciation of the scale of this threat grow. (Conclusion, Paragraph 62)

19. The ten key threats we outline above will rarely, if ever, present in isolation. Hostile actors are expected to target the UK economy along multiple vectors simultaneously. This poses particular challenges for an economy characterised by the private ownership of public risk, where the Government often lacks the tools to intervene rapidly across multiple sectors in response to a complex threat. (Conclusion, Paragraph 69)

20. We have heard through this inquiry that there is currently no shared space for industry and Government to simulate their response to combined attacks across multiple sectors, or to plan public and private investments that improve long-term resilience. This is dangerous. The National Exercising Programme, if implemented correctly over the course of this Parliament, is a step in the right direction. However, it is important that these exercises do not solely model the response to singular risks, but that to multiple simultaneous modes of attack. It is only through stress-testing complex simulations that vulnerabilities across the public and private sectors can be identified and addressed. (Conclusion, Paragraph 70)

21. The Government should conduct annual cross public sector-private sector exercises to specifically test the response to events in which multiple economic security risks manifest simultaneously. One example would be the scenario set out in the Strategic Defence Review: efforts to manipulate information, attacks on critical infrastructure, and wider attempts to disrupt the UK economy. These exercises could either form part of the National Exercising Programme or take place as a stand- alone wargame programme. (Recommendation, paragraph 71)

Transforming the economic security toolkit

22. The evidence we have received, and a comparison with our allies, leads us to conclude that the UK's economic security regime is no longer fit for the future. A whole-of-society approach must become the organising principle of Britain's economic security. (Conclusion, Paragraph 78)

23. The UK's approach to economic security shows less cross-government co-ordination than our most important international partners. The Government's approach is characterised by siloed thinking, a lack of adequate institutional support, and a reliance on strategies that are vulnerable to churn as ministers and governments change. The abolition of the National Security Council's Economic Security Sub-Committee leaves even less clarity as to how economic security will be factored in at the heart of Government decision-making. (Conclusion, Paragraph 86)

24. The Government must urgently reform Whitehall structures to improve cross-government co-ordination of economic security policy. We recommend that the Government learn from its own history, and following from the example of the 1920s it should:

- Appoint a cross-Government Minister for Economic Security, based in the Cabinet Office. This Minister should have responsibility for coordinating economic security related policy across Government, and be made a permanent member of both the National Security Council and the Economic Security sub-committee.
- Establish a new Office of Economic Security, that would bring together relevant expertise from across Whitehall, provide a platform for coordination with the private sector, and monitor the overall effectiveness of the UK's toolkit.
- Reinstate the Economic Security sub-committee of the National Security Council, with the Minister for Economic Security and the Secretary of State for Business and Trade as permanent members.
- Introduce legislation which would implement the recommendations of this report, and put the economic security related components of pre-existing strategies onto a statutory footing.

If the Government rejects the implementation of these measures, we recommend that it sets out in writing how it will improve cross- Government coordination, and ensure that its approach is driven by long-term goals. (Recommendation, paragraph 87)

25. Parliament and its committees must play a leading part in the national discussion around economic security, convening stakeholders from across sectors and advising Government on the strategic and cross- cutting steps needed to confront its challenges. Parliament, however, cannot hold the Government to account on its overall strategy for economic security if it is not able to access key information about the use of the UK's toolkit. (Conclusion, Paragraph 91)

26. The Government should commit to supporting select committee scrutiny of its approach to economic security. This should include a commitment to at least biannual public evidence sessions with senior Ministers and officials, and to complying with all reasonable requests for written information. This should include regular and comprehensive reports on the operation of the UK's economic security enforcement regimes, including sanctions, investment screening and export controls. (Recommendation, paragraph 92)

27. We acknowledge that some information may need to be provided in confidence, and we invite a dialogue between Government and Parliament to determine the appropriate parameters for this. (Recommendation, paragraph 93)

28. We reiterate the recommendation of our predecessor Committee, and recommend the Government explore ways of amending section 54 of the National Security and Investment Act 2021 to enable information relating to investment screening decisions to be shared with Parliament. (Recommendation, paragraph 94)

Diagnose a shared understanding of threats

29. The severity and breadth of the threats facing UK economic security will require a step change in information sharing between Government and the private sector. Businesses need accurate, up-to-date and actionable insights in order to plan investments and work constructively with government. We welcome the positive change that the new Economic Security Advisory Service could bring as a centre for advice, guidance and support to industry. However, it is essential that the Service does not operate solely as a Government-led initiative, but provides a forum for wider information sharing both between the public and private sectors, and within the private sector. (Conclusion, Paragraph 105)

30. The Government should increase its ambitions for the Economic Security Advisory Service to ensure that it acts as a centre for collaboration and information-sharing. Alongside its proposed functions, its remit should also encompass:

    - The functions of the previous Economic Security Public-Private Forum, with National Protective Security Authority (NPSA) briefings and research collaboration advice provided to businesses;
    - Forums for businesses to discuss challenges and risks with both the Government, and other businesses, in order to share best practice and identify emerging threats; and
    - A facility to provide tailored guidance and support regarding state-based threats.

    We recommend that the Government follow, and build on, the example of the National Cyber Security Centre in facilitating effective public-private co-operation. This platform should be organised by the new Office of Economic Security. (Recommendation, paragraph 106)

31. Emerging technologies have the potential to profoundly impact the UK's economic security. The UK's protective measures must keep pace with new risks, while not harming the competitiveness of its own technology sector. An accurate cross-Government understanding of the national security implications of future technologies will be essential, to mitigate harms and inform joined-up policymaking. (Conclusion, Paragraph 110)

32. We recommend that the creation of a cross-Government technology forecasting unit. This would lead an annual technology forecasting process, to support a co-ordinated response to technological change and the risk of new harms across the UK's economic security toolkit. This unit should be based within the new Office of Economic Security, to provide a cross-Government liaison point. (Recommendation, paragraph 111)

Develop sovereign capabilities

33. Economic security requires a clear-eyed understanding of which capabilities the UK needs to deliver for itself. Yet it is still not clear to us or, more importantly, to business investors what sovereign and asymmetric capabilities the Government aims to develop. So far, its approach has focussed on highlighting areas of economic strength, with no assessment of the areas in which it is over reliant on foreign-owned resources. (Conclusion, Paragraph 123)

34. The development of these sovereign capabilities is likely require an approach to public expenditure that is novel and not reflected in UK Government accounting principles. These principles evolved in a different era when our economic security was less perilous. (Conclusion, Paragraph 124)

35. The Cabinet Office should work with relevant sector bodies and Departments, to identify and publish a list of the 'sovereign capabilities' the Government wishes to develop for the nation. We recommend that the Government learns lessons from the approach taken under Japan's Economic Security Promotion Act in developing the UK list. It should include both sectors of strength, and areas in which the UK overrelies on foreign suppliers. The Government should then put forward clear long-term investment plans, supported by the National Wealth Fund, to encourage domestic production of priority capabilities. (Recommendation, paragraph 125)

36. We recommend that Government consult on the changes that may be required to the framework for managing public money in the face of challenges to economic and national security. This should include consideration of whether the tests underpinning managing public money

assessments adequately consider economic security imperatives and the benefits of securing both sovereign capabilities and critical supply chains. (Recommendation, paragraph 126)

Diversify critical supply chains

37. An understanding of supply chains is critical to a "whole-of-society" approach to economic security. While the new Supply Chain Centre will analyse key inputs, it will do so only in the specific context of the eight growth-driving sectors in the Industrial Strategy. We are concerned that this will only add to the current muddled picture, with new siloed understandings of sectoral vulnerabilities but no overall understanding of the UK's dependencies. The Government cannot take a strategic approach to sovereign capabilities without a clear understanding of the supply chains that support them. (Conclusion, Paragraph 132)

38. The Government should conduct a regular prioritisation exercise with industry and Parliament to identify the UK's critical supply chains. This assessment should combine data regarding critical raw material needs, and possible supply chain disruptions or dependencies, across the economy. From this, the Government should identify which supply chains require strengthening to build the UK's economic resilience. The results from the first of these exercises should be presented to Parliament within the next two years. (Recommendation, paragraph 133)

39. The Government's attempts to diversify supply chains, and to safeguard sources of critical minerals, will not be successful unless there is a long-term plan for the UK's supply chain. The forthcoming Critical Minerals Strategy is an opportunity to accelerate this work, and to set out clear priorities. The Government must however go further, and as a matter of policy pursue an alliance of free-trading democracies - such as Canada, which has considerable rare-earth assets - prepared to collaborate in securing mutual supply chains and critical mineral supplies and countering coercive economic behaviour. (Conclusion, Paragraph 140)

40. We recommend that the Government's forthcoming Critical Minerals Strategy:

- Sets specific targets for domestic production, recycling and processing.
- Clearly sets out the UK's approach to diversifying these supply chains through bilateral agreements with allies.
- Designates 'Critical Mineral Clusters' which would benefit from streamlined planning processes and support in accessing finance.

This should be accompanied by clear investment plans for both developing strategic stockpiles and diversifying these supply chains, co- financed by the National Wealth Fund. (Recommendation, paragraph 141)

Defend critical infrastructure, assets and sectors

41. Economic security cannot be achieved without cyber security. The spate of cyber-attacks in 2025 has underlined their potential to devastate not just targeted companies, but consumers and wider supply chains. We welcome the steps being taken to build the UK's cyber resilience, but these efforts need to be redoubled in light of recent events. (Conclusion, Paragraph 145)

42. The Government's Software Security Code of Practice is a useful first step in encouraging the take up of "secure by design" principles amongst software providers. Compliance with these principles, however, should be the minimum standard rather than a voluntary extra. More needs to be done to ensure that companies are not able to sell software that does not meet cybersecurity standards without being held to account for the damage it may then cause. (Conclusion, Paragraph 149)

43. We recommend that the Government introduce legislation that would mandate the standards set out in its Software Security Code of Practice. Enforcement agencies should be empowered to monitor compliance, and levy penalties against firms that do not adhere to these rules. (Recommendation, paragraph 150)

44. The cost of cyber resilience has increased significantly in recent years. Key upgrades to software and other IT services are often now made via payments to subscription services rather than one-off purchases, meaning that they are categorised as revenue rather than more tax- efficient capital expenditure. Improved cyber resilience is therefore having a bigger impact on company bottom lines. Businesses should not be forced to choose between resilience and profitability. Government must do more to incentivise investments in cyber security. (Conclusion, Paragraph 153)

45. The Government should amend the capital allowances regime to allow businesses to claim tax relief on subscription-based IT services that directly enhance operational resilience, such as cybersecurity software, legacy system upgrades, business continuity platforms and data protection solutions. A consultation on how this could best be achieved should be launched before the end of the year. (Recommendation, paragraph 154)

46. The UK Government will not be able to confront the threat posed by cyber-attacks without an accurate understanding of the scale of the problem. Currently large British companies are not required to report cyber-attacks. This is detrimental to national economic security. A full picture of these incidents is essential to not only the Government, but also to industry, helping both to better understand evolving threats and mitigations. (Conclusion, Paragraph 158)

47. We recommend that the Government consult on proposals for a mandatory malicious cyber incident reporting regime. (Recommendation, paragraph 159)

48. With greater and greater private ownership of public risk, there has never been a greater public interest in ensuring that private firms are able to prepare for disruption and recover quickly when it occurs. Risk is inevitable in private enterprise, and the public purse should not be substituted for an effective market. However, the increasingly complicated threat landscape means that the time is now ripe for Government to look again at the insurance market to ensure that it is functioning adequately. (Conclusion, Paragraph 164)

49. The Government should urgently consider expanding the scope of reinsurance schemes such as Pool Re to support private markets which enhance business resilience, particularly in respect of cyber threats. (Recommendation, paragraph 165)

50. A whole-of-society approach means recognising that firms are only as secure as the weakest link in their supply chain. A small company can play an economically critical role. SMEs require more support in their efforts to confront an ever more volatile and uncertain internationalenvironment. This support needs to go beyond new guidance and ensure that smaller firms have access to the necessary funding to implement security measures that improve both their resilience and security and that of the national economy. (Conclusion, Paragraph 170)

51. The Government should establish a dedicated SME Resilience Fund, administered by the Department for Business and Trade, to target support at enhancing the cyber resilience of smaller businesses. This fund should integrate with the Government's new Secure Innovation Reviews, by supporting businesses with the money required to make the improvements identified. (Recommendation, paragraph 171)

52. The UK economy needs large quantities of trusted investment. With the UK's growing capital requirements, the Government needs to strike the right balance between facilitating the flow of capital and blocking dangerous acquisitions. The Government is right to recognise that components of the UK's investment screening regime have become too burdensome. It

should also, however, go further and consider ways in which this tool can be modernised to encourage investment from trusted sources into critical sectors of the UK economy. (Conclusion, Paragraph 176)

53. We recommend that Government develop an accreditation scheme for providers of trusted capital, similar to the models used in the United States. Accredited investors should benefit from faster turnaround times within the UK's investment screening process, as well as continuous access to dedicated case management at all stages. A marketplace should then be created to connect these investors to companies in critical sectors of the UK economy. (Recommendation, paragraph 177)

Deter threats

54. Economy security requires not just resilience at home, but also effective deterrence of future threats. Improving the deterrent effect of trade sanctions and export controls requires greater transparency in enforcement outcomes. Breaches of either sanctions or export controls, even when resulting from error, are a serious matter, and businesses should not always be able to avoid the reputational harm of being publicly identified when they commit a breach. This is already recognised in the context of financial sanctions, where disclosure of breaches is already commonplace. (Conclusion, Paragraph 183)

55. Building on the 2022 recommendation of the Committees on Arms Export Controls, we ask the Government to clarify if there are any situations whatsoever in which it believes disclosure of the names of companies or individuals that enter into compound settlements for breaches of trade sanctions and strategic export controls would be lawful and in the public interest. Where such barriers may exist to limit disclosure, these should be removed. (Recommendation, paragraph 184)

56. Abuse of company registration has the potential to undermine the UK's deterrence regime. Companies House's new powers have the potential to make a significant difference in the fight against economic crime. In order to be effective, its implementation of these powers must focus on a significant improvement in the frequency of enforcement action. (Conclusion, Paragraph 187)

57. We recommend that Companies House steps up its disclosure of successful enforcement activity. The names of individuals who have been successfully prosecuted should be disclosed immediately following conviction, to both name and shame those involved in wrongdoing, and to highlight Companies House's progress in improving its approach to enforcement. (Recommendation, paragraph 188)

58. The UK's ability to deter economic threats depends upon agencies having the necessary staff in place to investigate wrongdoing. Currently, the UK depends on professionals committed to keeping the country safe, but today's pay scales mean that frontline enforcement agencies cannot attract the staff they need to adequately police the threat. Disparities with the private sector are significant - but so are disparities with the salaries of other public servants in similar ranks. (Conclusion, Paragraph 192)

59. We recommend that the Government urgently considers changing pay scales at organisations such as the National Crime Agency and Companies House, to ensure that salaries of mission critical staff keep pace with industry and fully reflect the indispensable work they do. (Recommendation, paragraph 193)

60. In today's volatile geopolitical climate, the UK must be able to defend itself against economic coercion from hostile actors. The Trade Strategy correctly recognises that today's trade remedies system does not adequately protect us against emerging economic threats. As economic coercion becomes more prevalent, the Government must go further and consider whether a new framework is now required to adequately protect the UK from coercive economic practices. (Conclusion, Paragraph 198)

61. The Government should establish a specific Anti-Coercion Instrument, and urgently launch a consultation on its design. Measures proposed should include a formal framework for responding to economic coercion and widening the available countermeasures to include restrictions on services trade, limitations on foreign direct investment and public procurement, and the suspension of intellectual property right protections. (Recommendation, paragraph 199)

Dovetail approaches domestically and internationally

62. Economic security must form a core component of the UK's international trading and geopolitical relationships. We reiterate our recommendations to deepen economic security co-operation with the United States, European Union and Asia-Pacific countries. In particular, a central pillar of the UK's trade strategy must be the establishment and maintenance of Western leadership in the race for technological superiority, particularly against China. Trade negotiations must identify opportunities to reinforce supply chain security through co-operation with allies, by exploring similar mechanisms to those being pursued in negotiations with the Republic of Korea. (Conclusion, Paragraph 208)

63. We welcome steps to establish economic security dialogues, but encourage these to develop in a more structured way. The ultimate aim of these endeavours should be an alliance of free trading democracies, leveraging bilateral and multilateral trading relationships to secure supply chains and counter coercive activities. (Conclusion, Paragraph 209)

64. The Government should prioritise in trade negotiations measures which will mutually benefit the economic security of the UK and key partners. The UK should proactively identify opportunities to align its economic security approach with those of trading partners. The Government should also commit to ongoing, structured dialogue with the United States, the European Union and Asia-Pacific countries on economic security, including supply chain resilience, investment security and technology leadership. (Recommendation, paragraph 210)

65. The UK has long benefited from the maintenance of an open international trading system. It must not acquiesce in the erosion of a global trading system that it is in our national interest to defend and to advance. The UK should continue to use its international influence to build support for renewed adherence to these rules. (Conclusion, Paragraph 213)

66. We recommend that the Government approach its engagement with multilateral institutions with a renewed focus on the promotion of the rules-based trading system. It should set out to us in writing, with examples, how it is doing so. (Recommendation, paragraph 214)

Formal minutes

Tuesday 11 November 2025

Members present

Liam Byrne, in the Chair

Dan Aldridge

Antonia Bance

John Cooper

Sonia Kumar

Justin Madders

Charlie Maynard

Matt Western

Toward a new doctrine for economic security

Draft Report (*Toward a new doctrine for economic security*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 216, read and agreed to.

Annex and Summary agreed to.

Resolved, That the Report be the Eleventh Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Adjournment

Adjourned till Tuesday 18 November at 2.00pm

Witnesses

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

Wednesday 7 May 2025

Helen Kennett, Director, Trade and Industrial Policy, Global Counsel; **Alexandra Kellert**, Associate Director, Control Risks; **Sir Simon Fraser**, Founding Partner, Flint Global Q1–37

Catherine Royle, Political Advisor to the Commander, NATO, Joint Force Command Brunssum; **The Lord Sedwill GCMG**, Former UK National Security Advisor; **Dr Francesca Ghiretti**, Research Leader, RAND Europe Q38–63

Mike Reid, Senior Partner, Frog Capital; **Nicole Kar**, Partner, Paul, Weiss; **Martin McElwee**, Partner, Freshfields Q64–87

Wednesday 21 May 2025

Mike King, VP Business Development and Government Relations, Cornish Lithium Limited; **Mr Paul Atherley**, Chairman, Pensana; **John Lindberg**, Policy & Government Affairs Principal, International Council on Mining and Metals (ICMM) Q88–115

Henrik Pederson, CEO, Associated British Ports; **Antony Walker**, Deputy CEO, techUK; **Trevor Hutchings**, Chief Executive, Renewable Energy Association; **Kevin Craven**, CEO, ADS Group Q116–144

Chris Parker MBE, Director, Government Strategy, Fortinet; **Mr Zeki Turedi**, Field Chief Technology Officer, Europe, CrowdStrike; **Simon Thomas**, CEO, Paragraf; **Dr Brendan Casey**, CEO, Kelvin Nanotechnology Ltd Q145–164

Tuesday 8 July 2025

Archie Norman, Chairman, Marks and Spencer; **Nick Folland**, General Counsel, Marks and Spencer; **Victoria McKenzie-Gould**, Corporate Affairs Director, Marks and Spencer Q164–191

Dominic Kendal-Ward, Group Secretary and General Counsel, Co-op Group; **Rob Elsey**, Group Chief Digital Information Officer, Co-op Group Q192–213

Professor Ciaran Martin, Professor of Practise in the Management of Public Organisations, Blavatnik School of Government, University of Oxford; **Jamie MacColl**, Senior Research Fellow, Cyber and Tech, RUSI; **Katharina Sommer**, Group Head of Government Affairs and Analyst Relations, NCC Group Q214–234

James Babbage, Director General (Threats), National Crime Agency; **Richard Horne**, Chief Executive Officer (CEO), National Cyber Security Centre; **Andrew Gould**, Detective Chief Superintendent for Cyber and Economic Crime, City of London Police, National Cybercrime Programme Lead, National Police Chiefs' Council Q235–258

Wednesday 9 July 2025

Rt Hon Douglas Alexander MP, Minister of State for Trade Policy and Economic Security, Department of Business and Trade; **Rt Hon Pat McFadden MP**, Chancellor of the Duchy of Lancaster, Cabinet Office; **Philippa Makepeace**, Director, Geopolitics and Economic Security, Department for Business and Trade; **Jonathan Black**, Deputy National Security Adviser (Economics), Cabinet Office, Director General for European & Global Issues, Cabinet Office Q259–315

Published written evidence

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

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

1	ADS Group	ECO0002
2	Altana	ECO0011
3	Beckton Dickinson UK	ECO0032
4	Boardwave	ECO0020
5	Bird, Jenny (Campaign Manager, Grantham Institute, Imperial College); Della Croce, Raffaele (Senior Research Fellow , Centre for Climate Finance & Investment, Imperial College Business School); and Gambhir, Dr Ajay (Director of Systemic Risk Assessment, Accelerator for Systemic Risk Assessment (ASRA); Grantham Institute, Imperial College London)	ECO0022
6	Boff, Professor Jonathan (Professor of Military History, University of Birmingham)	ECO0008
7	British Private Equity and Venture Capital Association (BVCA)	ECO0013
8	Campaign Against Arms Trade	ECO0031
9	Centre for Economic Security	ECO0003
10	Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI)	ECO0012
11	Centre for Inclusive Policy and UK Trade Policy Observatory	ECO0014
12	Chatham House	ECO0018
13	Coalition on Secure Technology	ECO0015
14	Council on Geostrategy	ECO0019
15	Germond, Professor Basil (Chair in International Security, Lancaster University)	ECO0026
16	Hibbert, Mr Dylan (Director, Panaco)	ECO0005
17	Holliday, Jamie (Student, Edge Hill University); and Murphy, Charlie (Student, Edge Hill University)	ECO0007

18	Jackson, Dr Karen (Reader in Economics, University of Westminster); and Shepotylo, Dr Oleksandr (Senior Lecturer in Economics, Aston University)	ECO0009
19	Kelvin Nanotechnology Ltd	ECO0035
20	Lai, Dr Daniela (Senior Lecturer in International Relations , Royal Holloway, University of London)	ECO0024
21	Lenihan, Dr Ashley (Professor of the Practice of International Affairs, Georgetown University)	ECO0025
22	Lewis, Professor Michael (School of Management, University of Bath)	ECO0027
23	Millar, Alistair (President, Fourth Freedom Forum)	ECO0029
24	Moore, Dr Kathryn, (Senior Lecturer in Critical and Green Technology Metals, Camborne School of Mines, University of Exeter); and Storrie, Dr Bridget (Teaching Fellow, The Institute for Global Prosperity, University College London)	ECO0034
25	Oxford China Policy Lab	ECO0016
26	Procter, M	ECO0010
27	RAND Europe	ECO0021
28	Saferworld	ECO0023
29	Searle, Dr. Nicola (Reader (Associate Professor), Goldsmiths, University of London)	ECO0006
30	Stavrianakis, Professor Anna (Professor of International Relations and Director of Research and Strategy , University of Sussex and Shadow World Investigations)	ECO0017
31	The Centre for Finance and Security at the Royal United Services Institute	ECO0036
32	TheCityUK	ECO0028
33	techUK	ECO0030

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
10th	US Economic Prosperity Deal	HC 1306
9th	Draft Legislative Reform (Disclosure of Adult Social Care Data) Order 2025	HC 1140
8th	Export led growth: Trade with the Asia-Pacific region	HC 1048
7th	Industrial Strategy	HC 727
6th	How to strengthen UK-EU relations: Policy Priorities for the Summit	HC 908
5th	How to strengthen UK-EU relations	HC 814
4th	Post Office Horizon scandal redress: Unfinished business: Government response	HC 778
3rd	Make Work Pay: Employment Rights Bill	HC 370
2nd	Priorities of the Business and Trade Committee	HC 423
1st	Post Office and Horizon scandal redress: Unfinished business	HC 341
5th Special	Export led growth: Trade with the Asia-Pacific Region: Government Response	HC 1324
4th Special	Industrial Strategy: Government Response	HC 1305
3rd Special	How to strengthen UK-EU relations: Policy Priorities for the Summit: Government Response	HC 1267
2nd Special	Post Office Horizon scandal redress: Unfinished business: Government response	HC 969
1st Special	Make Work Pay: Employment Rights Bill: Government response	HC 932