

26 September 2025

Chair of the Business and Trade Sub-Committee on Economic Security, Arms and Export Controls
House of Commons
London
SW1A 0AA

ANALYSIS SUBMITTED BY THE CENTRE FOR FINANCE & SECURITY AT RUSI

Dear Mr Byrne,

Following discussions with the Committee team, it was agreed that the [Centre for Finance & Security \(CFS\) at the Royal United Services Institute \(RUSI\)](#) would submit analysis on how the UK's approach to economic security compares with that of key international counterparts. Please find enclosed a Word document which presents the findings in a high-level comparative table.

The international comparison highlights that, while the UK has made important progress in operationalising economic security, its approach remains more fragmented than some of its peers. The UK has developed an impressive set of strategies – including the Industrial Strategy 2025 and its associated sectoral plans, the Critical Minerals Strategy and cyber security framework – but unlike Japan's Economic Security Promotion Act or the EU's European Economic Security Strategy, it does not yet have a single legislative, strategic or institutional anchor. Instead, responsibilities are spread across departments, with coordination achieved largely through policy documents that tend to be replaced or rewritten by successive governments, limiting long-term continuity.

By contrast, Japan has embedded economic security in statute, created a dedicated ministerial role, and combined regulatory certainty with substantial financial support for emerging technologies. Although the US also uses a distributed governance model similar to the UK (with several agencies handling overlapping elements of economic security), it has leveraged executive action and major industrial funding to act decisively on critical mineral production and frontier technologies. The EU's approach may seem slow-moving by comparison, but it is leveraging its regulatory power and single market to align member states on supply chains, raw materials and export controls.

The overarching strategic takeaway is that economic security is increasingly being treated as a system-wide organising principle, rather than a collection of siloed sectoral initiatives. The UK's policy challenge is therefore twofold: first, to consolidate its current patchwork of strategies into a more coherent and enduring governance framework, ideally with statutory backing, and second, to scale up its investment and coordination mechanisms if it is to keep pace internationally. Without increased institutional

permanence and financial scale, the UK risks being seen as a policy follower rather than a leader – strong in analysis and strategy, but with less institutional authority and financial firepower than its allies.

Yours sincerely



Tom Keatinge
CFS Director
tomk@rusi.org

Encl: Word document 'CFS at RUSI_DBT economic security analysis'

About CFS at RUSI

Since its formation in 2014, CFS has focused on matters at the intersection of finance and security. CFS uses its evidence-based research and convening power to support policymakers, operational agencies and the private sector across the globe, as well as undertaking extensive engagement with multilateral bodies. CFS's '[Sanctions, State Threats and Economic Security](#)' research programme examines the financial dimension of state threats, the expanding focus on economic security, and the weaponisation of finance as a tool of international statecraft in an increasingly fragmented geopolitical landscape.

In 2024, CFS established a [European Economic Security Taskforce](#) (the Taskforce) bringing together over 40 international policymakers from member states, EU institutions and key allies, geoeconomic academics, security experts and private-sector representatives. Three Taskforce reports are [available online](#), which examine the conceptual and practical challenges of economic security policymaking; the systems and structures necessary to develop robust economic security priorities; and the need to build greater strategic alignment between the public and private sectors to achieve economic security ambitions.

CFS has convened economic security events and workshops in collaboration with a wide range of international stakeholders, in addition to engaging with the current UK government. In March 2025, CFS Director [Tom Keatinge](#) participated in the Business and Trade Sub-Committee on Economic Security's expert engagement event, and CFS Research Fellow [Eliza Lockhart](#) was invited to present the Taskforce's findings at the inaugural UK Government Economic Security Overseas Network Conference.

ANALYSIS SUBMITTED BY THE CENTRE FOR FINANCE & SECURITY AT RUSI

Executive Summary

A comparative review of the UK, US, EU and Japan shows that the UK's approach to economic security is strategically active, but less institutionally consolidated than some of its peers. The UK has developed an impressive set of strategies that cover elements of economic security – including the Industrial Strategy 2025 with eight sector plans (notably the Digital and Technologies Sector), a suite of technology-specific strategies (AI, quantum, semiconductors, engineering biology, cyber), and initiatives on supply chains, critical minerals, and investment screening. This policy-driven flexibility allows the UK to adapt quickly to emerging challenges, but the reliance on strategies rather than a legislative framework makes their longevity dependent on political cycles. This stands in contrast to Japan, which has built a durable economic security framework through the Economic Security Promotion Act (ESPA), established a dedicated ministerial role and provides substantial financial support for emerging technologies. The US combines legislative and executive action with large-scale industrial investment to drive its agenda forwards, although recent political shifts have raised questions about the predictability of future policy direction. The EU is using its regulatory power and single market to create a long-term, rules-based approach to supply chain resilience, critical raw materials, and technology protection, but its reliance on consensus among member states can limit agility and delay responses to fast-moving threats.

Key Takeaways

1. Institutional permanence is now a strategic differentiator

One of the UK's structural weaknesses is its reliance on policy papers and strategies that are frequently replaced by new governments – a pattern of 're-inventing the wheel' that became apparent in the literature review. By contrast, legislative frameworks in Japan and the US give their economic security agendas continuity beyond electoral cycles, enabling long-term industry and investor confidence. In the emerging era of economic security competition, the ability to plan, invest and act across decades rather than parliaments is becoming a source of strategic strength.

2. Scale and industrial policy are shaping leadership

The US is translating its economic security agenda into industrial power through the CHIPS and Science Act, massive quantum and AI funding, and broad executive actions. This scale of investment not only secures domestic capability but also shapes global standards and supply chains – though arguably creating unfair market distortions. Japan, though smaller, is matching ambition with substantial semiconductor and technology subsidies. By comparison, the UK's initiatives remain strategically coherent but comparatively financially constrained, limiting its ability to influence global production networks and technology ecosystems.

3. Regulatory coherence underpins resilience

The EU's rules-based model — with an overarching economic security strategy, supported by economic security risk assessments, legislation, regulation and recommendations — shows how a regulatory regime can both manage risk and mobilise private sector innovation. The UK's more flexible mix of sectoral strategies allows for faster policy adjustment when geopolitical risks arise but provides less certainty, potentially weakening business confidence and long-term supply chain diversification.

4. Cyber security and emerging technology policy are converging globally

All four actors now treat cyber security as an emerging technology. The US integrates critical and emerging technologies into its National Cybersecurity Strategy; Japan has taken a decisive step with its Active Cyber Defense Law; and the EU embeds cyber security as an integral part of its aspirations for technology innovation through its Digital Decade policy programme. The UK recognises cyber as a frontier technology and is moving forward with a new Cyber Security and Resilience Bill and an updated National Cyber Strategy – all positive steps – although its fragmented governance model may slow the integration of cyber resilience with wider economic security priorities.

Strategic Significance for the UK

The comparison underscores that economic security is no longer just a set of sectoral initiatives – it is an organising principle of state power. Nations that anchor their approach in law-backed, long-term governance structures are better able to sustain direction, mobilise investment and shape global standards. The UK's breadth of expertise is a clear asset but by continuing to rely on policy papers vulnerable to political turnover, the UK risks losing strategic continuity at precisely the moment when economic security demands decades-long foresight. Meanwhile, competitors are combining institutional durability, regulatory certainty and industrial-scale funding to build advantage in supply chains, frontier technologies and cyber resilience. Unless the UK evolves beyond its current policy-fragmented model, it may remain a strategic follower – agile in analysis and narrative but lacking the permanence and financial scale that is increasingly defining global economic security leadership.

- **Consolidate and codify:** Move from a patchwork of sector strategies to a statutory economic security framework that endures across governments.
- **Scale investment:** Pair strategic intent with industrial-level funding to compete for global leadership in semiconductors, quantum, AI and other frontier technologies.
- **Integrate cyber and tech policy:** Ensure the National Cyber Strategy refresh is fully aligned with emerging technology protection and promotion.
- **Partner with the private sector:** Consider EU-style risk assessment cycles and clearer channels for information exchange to give government and business a shared understanding of vulnerabilities.

Table: Economic Security Approaches – An International Comparison

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
<i>Overarching</i>	Definition	No overarching definition, but the Integrated Review 2021 links the UK's economic security to combatting increasing state-based threats, strengthening cyber security, and building national resilience. The National Security Strategy 2025 states “economic security is national security” and links economic security to building resilience through domestic capacity building, diversification and strategic international partnerships; defending against foreign state threats and malign investment; and nurturing the UK's industrial, scientific and technological base.	No overarching definition. The 2017 US National Security Strategy states “economic security is national security” and a 2021 White House fact sheet emphasizes resilient and secure supply chains to address trade disruptions, natural disasters, and actions by foreign competitors and adversaries. In 2021, the Homeland Security Act 2022 was amended, with 6 U.S. Code § 474(c)(2) defining economic security as: “the condition of having secure and resilient domestic production capacity, combined with reliable access to global resources necessary to maintain an acceptable standard of living and to protect core national values”.	No overarching definition, but the European Economic Security Strategy (2023) provides four “broad and non-exhaustive categories of risks” facing European economies – supply chain disruptions, critical infrastructure, technology leakage and economic coercion. The strategy's approach to these risks is based on three pillars – promote (EU competitiveness), protect (through mitigating measures) and partner (with likeminded countries).	Japan's National Security Strategy 2022 defines economic security as “to ensure Japan's national interests, such as peace, security, and economic prosperity, by carrying out economic measures ... in the face of various threats”. This was expanded upon by the Economic Security Promotion Act 2022, which has four pillars of “economic measures related to ensuring security” – strengthening supply chains for critical products, ensuring stable provision of essential infrastructure services, promoting the development of specified critical technologies, and prohibiting the disclosure of selected patent applications.

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
	Economic security strategy and law	No overarching strategy. Economic security issues are covered by various strategies and legislation, including but not limited to: Export Control Act 2002 ; Dual-Use Regulation (EC) No. 428/2009 ; Sanctions and Anti-Money Laundering Act 2018 ; Integrated Review 2021 ; National Security and Investment Act 2021 ; National Security Strategy 2025 ; Industrial Strategy 2025 ; Trade Strategy 2025 .	No overarching strategy, but an extensive economic security toolkit – from well-established mechanisms, such as the foreign investment scheme managed by the Committee on Foreign Investment in the US (established in 1975); to newer initiatives, such as the CHIPS and Science Act 2022 that provides incentives to produce semiconductors in the United States.	An overarching strategy – the European Economic Security Strategy (see the definition section above).	An extensive toolkit supported by two key pieces of legislation: (i) Economic Security Promotion Act 2022 , which is implemented/ supported by the Ministry of Economy, Trade and Industry’s “ Action Plan to Strengthen Industrial and Technological Basis for Economic Security ” (May 2025); and (ii) Critical Economic Security Information Act 2024 .
	Governance	Economic security governance is not consolidated within a single agency. The closest to an overarching agency on economic security issues is the UK National Security Council , which considers economic security as part of its boarder strategic approach to national security, but its Economic Sub-Committee was abolished .	Responsibility for economic security governance is distributed across multiple agencies, rather than being vested in one central authority. These agencies include the US National Security Council , the Department of Homeland Security (Trade and Economic Security) , and the Office of Strategic Industries and Economic Security (within the US Department of Commerce).	Economic security primarily falls within the remit of the Directorate-General for Trade and Economic Security for the European Commission (DG TRADE). However, most European Commission Directorates-General involve elements of economic security and there is a lack of integrated horizontal governance structures to ensure coordination and oversight.	Japan has undertaken significant institutional reforms to ensure that economic security policies are coordinated across government. These include establishing: an economic division within the Japanese National Security Secretariat and similar units within key ministries; a dedicated ministerial portfolio for economic security; and a Council for the Promotion of Economic Security chaired by the Prime Minister.

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
<i>Regimes</i>	Sanctions (financial and trade)	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.	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 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.	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.

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
	Investment screening (inbound and outbound)	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.	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.	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.	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.

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
	Export controls (military, traditional, dual-use and advanced tech)	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.	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.	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.	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.

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
	Supply chains	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.	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.	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.	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.

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
	Critical minerals	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.	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.	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.	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 (see the columns to the right for details of these agreements).

TOPIC	DIMENSION	UK	UNITED STATES	EUROPEAN UNION	JAPAN
	Emerging technologies	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 (hyperlinked above). 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.	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.	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.	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.

