www.rusi.org

Conference Report

RUSI European Economic Security Taskforce

Meeting 3: Precision, Pragmatism and Partnership

Eliza Lockhart

Conference Report

194 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.

RUSI Conference Report, August 2025

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

RUSI European Economic Security Taskforce
Meeting 3: Precision, Pragmatism and Partnership

Introduction

Economic security has rapidly become a central pillar of domestic and international policy agendas. Its rise reflects escalating geopolitical tensions and a growing recognition of systemic vulnerabilities within the global trade and financial systems. Russia's war in Ukraine, the ongoing instability in the Middle East, and an intensifying strategic rivalry between the US and China have all underscored the security risks embedded in global economic interdependence. At the same time, recent worldwide shocks – from pandemic-induced supply chain disruptions to financial market volatility – have exposed the fragility of systems long assumed to be stable and self-correcting.

In response, governments are increasingly reorienting their economic strategies through a security lens, with greater emphasis on the resilience of strategic supply chains, protection of critical infrastructure, and tighter controls over dual-use technologies. At the national level, this approach is widely seen as requiring a careful balance between remaining open to global markets and diversifying trading partners while also mitigating exposure to coercive dependencies and preserving strategic autonomy. Internationally, many observers note a broad shift away from rules-based multilateralism and liberalised trade towards a more fragmented landscape shaped by protectionism and the growing securitisation of economic relations.

To help navigate this complex and evolving terrain, in 2024 the Centre for Finance and Security (CFS) at RUSI established a European Economic Security Taskforce (the Taskforce).[1] CFS is uniquely positioned to deliver this initiative because its team (based in London and Brussels) has extensive experience analysing issues

1. RUSI, 'European Economic Security Taskforce', <https://www.rusi.org/explore-our-research/projects/european-economic-security-taskforce>, accessed 7 July 2025.

at the intersection of finance and security, as well as a deep understanding of public sector policymaking and private sector practicalities.

To convene the Taskforce, CFS drew on its cross-disciplinary expertise and multi-jurisdictional network to bring together over 40 policymakers, security experts, business representatives and geoeconomic academics.[2] Taskforce members include member state economic security policymakers, alongside experts from the European Council, the Directorate General for Trade and Economic Security of the European Commission (DG TRADE), the European External Action Service, and the EU Institute for Security Studies. The Taskforce also includes representatives from NATO and key EU allies, including Australia, Japan, Norway and the UK.

This report has three main sections. First, it sets out CFS's understanding of economic security by outlining its economic security framework, which has been developed through Taskforce discussions. Second, it provides a brief overview of the initial work of the Taskforce, highlighting the key finding that strong and sustainable public–private partnerships (PPPs) are essential to implementing effective economic security strategies. The pressing need to understand PPP best practice in this context is what is driving the next phase of the Taskforce. To advance this work – and in light of Denmark assuming the EU Council Presidency for the second half of 2025 – CFS partnered with Danish Taskforce members to hold an economic security workshop in Copenhagen in June 2025. The final section of the report summarises the key observations from that workshop and integrates them into CFS's broader thinking on economic security PPPs.

The CFS Economic Security Framework

Economic security is a contested topic and defining what it means is the necessary first step for any meaningful analytical or policy effort. Drawing on Taskforce meeting discussions, CFS has developed an economic security framework that outlines how the term is conceptualised and applied in its work. Presented in Figure 1, this framework includes a definition, a description of its two types of application, and an explanation of how it is operationalised across three layers of impact: risks, levers and context.

The framework is best explained through a simplified real-world example. Consider the critical mineral of lithium – an essential component in batteries that are used in a wide range of technologies, including electric vehicles,

2. Taskforce members contribute their expertise in a personal capacity and do not represent their respective organisations or countries.

smartphones and renewable energy storage systems. Australia is the world's largest supplier of lithium, accounting for more than half of the total global output.[3] While it is clearly in Australia's economic interests to protect and promote its production of lithium, there are also significant security implications.

To start an economic security analysis, **Layer 1** of the framework requires the collection of data to assess the various security risks and economic opportunities involved with the relevant activity, in this case, mining a critical mineral. For instance, while lithium can help accelerate Australia's green energy transition, it also raises concerns about supply chain vulnerabilities and economic dependencies.

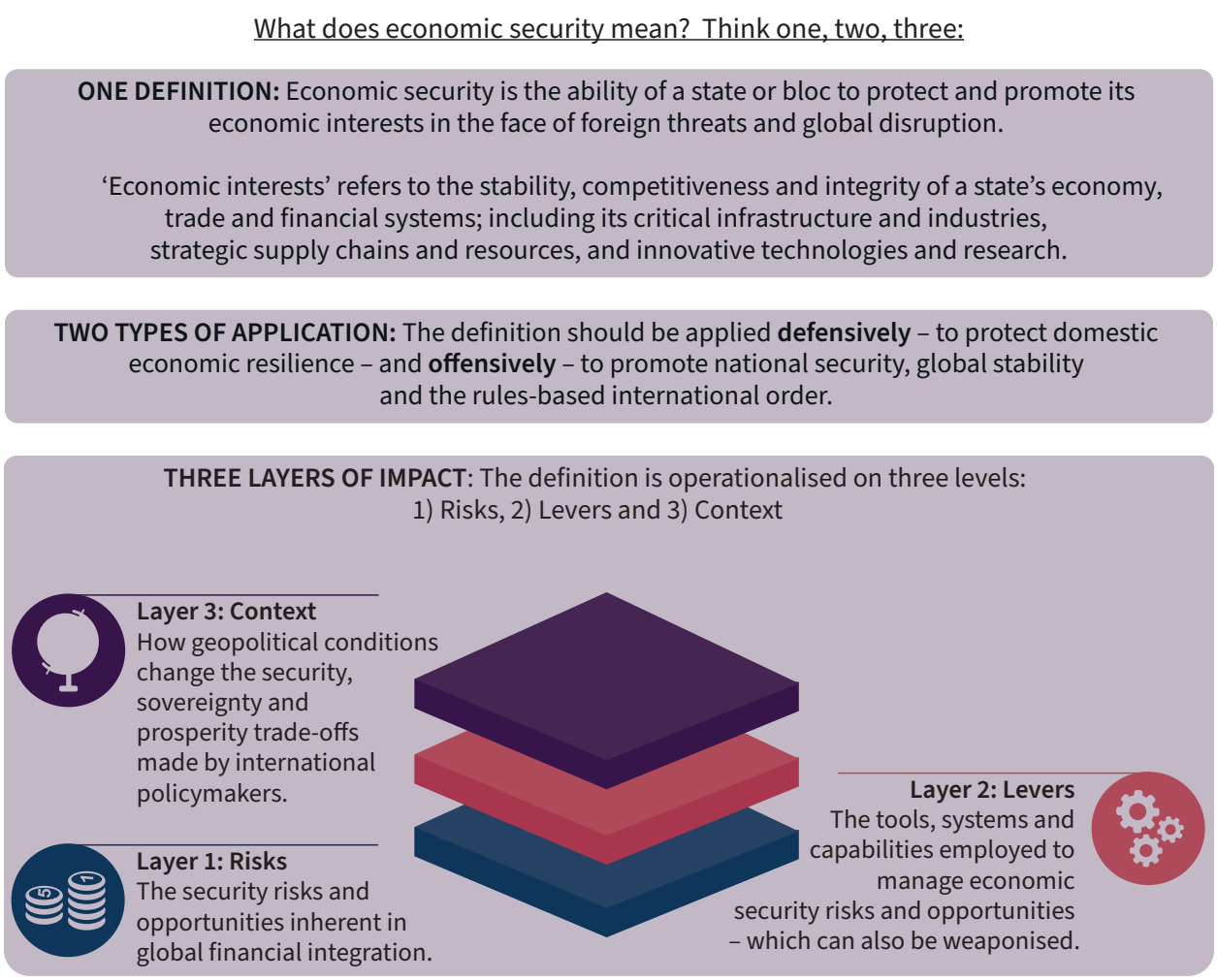
Layer 2 focuses on what levers are available to a government to manage these risks and opportunities, as well as the trade-offs involved. For example, as 96% of Australian lithium was exported to China in 2022, it has been suggested that Australia should build onshore lithium processing facilities.[4] While this could enhance domestic supply chain resilience and reduce Australia's exposure to Chinese economic coercion, it would also require substantial public and private investment.[5]

Layer 3 applies the broader geopolitical context to this decision-making process. As the US–China strategic competition intensifies, Australia is forced to navigate increasing pressure from both partners. Diversifying or 'de-risking' lithium exports could trigger economic retaliation from China, while inaction may strain Australia's security partnership with the US.[6] Layer 3 captures these contextual factors and their implications for national decision-making.

This example illustrates how the framework is intended to not only clarify how CFS defines economic security, but also provide a foundation for the Taskforce's mission, which is to translate broad concepts into actionable strategies through evidence-based analysis and engagement with government, business and security stakeholders.

3. Andrew Tunnicliffe, 'Australia Makes Moves to On-Shore Lithium Operations', *Mining Technology*, 27 December 2024, <https://www.mining-technology.com/features/australia-makes-moves-to-on-shore-lithium-operations/>, accessed 9 July 2025.
4. Marina Yue Zhang, 'Global Lithium Supply and Australia's Role', Australian Institute of International Affairs, 15 June 2023, <https://www.internationalaffairs.org.au/australianoutlook/global-lithium-supply-and-australias-role/> accessed 9 July 2025.
5. Note, this is one of the actions Australia has decided to take as part of its Critical Minerals Strategy 2023–2030. See Australian Government, Department of Industry, Science and Resources, 'Critical Minerals Strategy 2023–2030', 7 July 2023, <https://www.industry.gov.au/publications/critical-minerals-strategy-2023-2030>, accessed 9 July 2025.
6. Alexander Korolev and Fengshi Wu, 'Australia's Critical Minerals Strategy amid US–China Geopolitical Rivalry', *RUSI Commentary*, 22 April 2024, <https://www.rusi.org/explore-our-research/publications/commentary/australias-critical-minerals-strategy-amid-us-china-geopolitical-rivalry>, accessed 8 July 2025.

Figure 1: The CFS Economic Security Framework



Source: The author.

Key Taskforce Finding – Importance of PPPs

At the outset, the objective of the Taskforce was to convene a cross-section of experts to examine how economic security is being integrated into policymaking at the member state and EU level, and what barriers are preventing effective implementation. Put simply, the first phase of the Taskforce involved looking at what is working and what is not. Two meetings were held during this initial phase, with reports of their findings publicly available.[7]

The first Taskforce meeting focused on the consequences of the lack of clarity around what economic security means, both within national ministries and at the EU level. Taskforce members noted how this conceptual ambiguity has contributed to siloed approaches and fragmented policymaking. They also observed that the absence of a shared understanding of economic security has prevented the articulation of clear policy objectives by member state and EU policymakers. This, in turn, has undermined efforts to collect quality data, prioritise vulnerabilities, build consensus on proportional interventions, and engage with the private sector in a coordinated manner.

The second Taskforce meeting built on these findings by exploring what systems and structures could produce robust European economic security priorities, policies and partnerships. Many Taskforce members emphasised the need for horizontal governance structures within national administrations and across EU institutions to develop and align clear economic security goals. Such interagency coordination would not only improve internal coherence, but could also serve as a foundation for more effective communication, information sharing and collaboration with the private sector.

The consensus from both meetings was clear – the success or failure of economic security strategies will largely depend on strategic alignment between the public and private sectors, which necessarily requires the private sector to be meaningfully engaged as an active partner. However, at present the relationship between the sectors on economic security issues remains disjointed. Businesses are on the front line of economic warfare, yet are often frustrated by inconsistent

7. For the report from the first meeting, see Eliza Lockhart, 'RUSI European Economic Security Taskforce, Meeting 1: The Conceptual and the Concrete', RUSI Conference Report, 18 October 2024, <https://www.rusi.org/explore-our-research/publications/conference-reports/rusi-european-economic-security-taskforce-meeting-1-conceptual-and-concrete>, accessed 14 July 2025. For the report from the second meeting, see Eliza Lockhart, 'RUSI European Economic Security Taskforce, Meeting 2: Systems and Structures', RUSI Conference Report, 7 February 2025, <https://www.rusi.org/explore-our-research/publications/conference-reports/rusi-european-economic-security-taskforce-meeting-2-systems-and-structures>, accessed 14 July 2025.

regulatory requirements, limited communication from governments, and insufficient consultation on policies that significantly affect their operations. Conversely, policymakers must develop cross-cutting economic security strategies while having limited visibility into supply chain vulnerabilities, restricted access to commercially sensitive data, and dealing with businesses that prioritise profit above security.

These recurring challenges have informed CFS's objective for the second phase of the Taskforce – to bring together business leaders, professional service providers and policymakers to explore best practice for PPPs in the context of economic security. In doing so, CFS aims to avoid the common pitfalls of economic security analysis – drifting into blue-sky policy thinking or becoming immersed in technical and industry-specific detail – by exploring a sector-agnostic framework for effective economic security PPPs. CFS launched this second phase of the Taskforce with a workshop focused on Danish economic security.

Copenhagen Workshop

Denmark's assumption of the EU Council Presidency in July 2025 presented an ideal opportunity to convene leading government and business representatives recognised for their expertise on economic security issues. In partnership with the Danish Ministry of Foreign Affairs, Danish Industry and Think Tank Europa, CFS convened an economic security workshop in Copenhagen on 10 June 2025.

Participants included delegates from the Danish Ministry of Foreign Affairs and DG TRADE, as well as key actors from Denmark's private sector – spanning transport, shipping and logistics, supply chain services, power cables, wind power, mining technology, and defence. Specialists from banking, finance, engineering, and risk and compliance consulting also contributed valuable perspectives.[8]

The following sections are organised thematically around three core concepts that are necessary for improved coordination between public and private sectors on economic security: precision, pragmatism and partnership. The analysis presented synthesises insights gained from both the workshop and CFS's ongoing work in this field.

8. The workshop was held on a non-attributable basis and the names and affiliations of participants are not disclosed. Moreover, participants were not required to establish agreed positions and, therefore, this report does not necessarily represent the views of all participants.

1. Precision

The Copenhagen workshop opened with both the Danish government and business representatives commenting that there does not seem to be a widely agreed definition of economic security. Many participants expressed that they had an intuitive understanding of the concept, along the lines of: 'we know it when we see it'. However, there was general agreement that this conceptual ambiguity was an increasingly significant barrier to effective economic security collaboration between the public and private sectors.

At the European level, the EU Economic Security Strategy stops short of offering a concrete definition. Instead, it identifies four 'broad and non-exhaustive categories of risks' facing European economies.[9] Although participants found these categories helpful, many viewed them as overly broad, with one workshop participant remarking that the EU appears to define economic security as 'any risks that emerge through economic linkages with other partners'. Several private sector participants cautioned that such a wide framing of economic security without clear objectives could result in excessive intervention and securitisation, echoing concerns raised in previous Taskforce meetings.[10]

Defining the scope and priorities of economic security policy is understandably challenging given its cross-cutting nature, which spans the trade, economic, industrial, energy, research, foreign and national security policy domains. One participant likened it to a complex game of 'connect the dots' – if the connections are drawn too widely, it becomes nearly impossible to prioritise threats or craft proportionate interventions. On the other hand, a narrow focus on specific sectors or an over-emphasis on growth may overlook systemic vulnerabilities in integrated global markets and expose countries to undue risk.

As one participant observed, this process of conceptualising what economic security means in today's geopolitical environment 'is very much still a work in progress' because 'despite there being a lot of academic discussion, there is very little practical experience in how to manage this'. To get the balance right, the participant suggested that 'governments need to apply greater precision in their economic security analysis, risk identification, and responses'. Precision, in this context, does not imply rigidity, but refers to clarity of concept, strength of objectives and quality of evidence.

9. European Commission, 'Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy"', JOIN/2023/20 final, 20 June 2023, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2023:20:FIN>, accessed 16 July 2025.
10. Lockhart, 'RUSI European Economic Security Taskforce, Meeting 1', p. 4.

The call for precision across economic security analysis, risk identification and responses resonated strongly with others and was explored further, as detailed below.

Analytical precision requires clarity about what policymakers are trying to protect. From a Danish perspective, this includes upholding open trade, free and fair competition, a well-functioning internal market and good investment conditions in Europe. At the same time, governments may need to use tools that undermine competitiveness but are necessary to safeguard critical infrastructure and technologies. Analytical precision ensures that such decisions are founded on a clear understanding of which assets, technologies, capabilities, and market conditions are vital to long-term security and prosperity.

Risk identification precision requires both the ability to recognise threats and to assess their strategic relevance. As one participant observed, 'we can easily see risks everywhere'. Precision in risk identification involves undertaking thorough risk analysis to understand the specific vulnerabilities within sectors, the nature and severity of the risks, their broader implications, and how to apply mitigation measures with minimal commercial disruption. Grounding these assessments in operational realities and security considerations requires close collaboration between the public and private sectors, as well as between economic and security specialists.

Response precision is essential to ensuring that solutions are tailored to the specific context. Economic security challenges rarely lend themselves to one-size-fits-all solutions. For example, when addressing risks related to imported critical components in wind turbines, should the response involve export controls, anti-coercion instruments and stricter procurement rules? Or should governments prioritise domestic production, investment in innovation, and collaboration with like-minded partners? In most cases, workshop participants observed that a strategic mix of tools is needed, applied in a proportionate and consultative manner. While today's environment may demand more intervention than in the past, precision ensures that such action is measured, targeted and avoids blunt or counterproductive responses.

Box 1: Precision in Brief

- **Conceptual clarity is lacking**: Broad definitions of economic security without clear objectives make coordinated policy responses more difficult and may lead to excessive securitisation.
- **Analytical precision is fundamental**: A clear understanding of what needs to be protected – such as open markets, critical infrastructure and technologies, and innovation capacity – is essential for effective policy.
- **Risk identification must be targeted**: With security risks emerging across all sectors, precision is needed to distinguish between theoretical or low-grade threats and those requiring urgent attention and mitigation.
- **Tailored, proportionate responses are essential**: One-size-fits-all solutions are ineffective; instead, governments should employ a strategic mix of tools based on context-specific assessments and consultation with the private sector.

2. Pragmatism

The second key concept to emerge from the Copenhagen workshop was pragmatism. There was a strong consensus on the need for a 'mindset shift' in both the public and private sectors to turn economic security from abstract principle into actionable policy. Greater precision will enable greater pragmatism, but clarity in analysis, risk identification and response is not enough. It must be accompanied by a shift in culture, incentives and operating systems across business and government. These complementary shifts are explored in more detail below.

Private Sector Mindset Shift – from Opportunity-First to Risk-Informed

For the private sector, embracing economic security requires moving beyond a narrow focus on aggressively capturing market opportunities towards integrating security risks into commercial strategy. As several participants noted, many industries began this shift following the supply chain shocks triggered by the Covid-19 pandemic. However, for the majority of businesses – particularly small and medium enterprises (SMEs) – much work remains.

This involves treating economic security not as an externality to be managed by government, but as a core business concern. As one risk and compliance specialist put it, companies must spend 'a portion of profits on securing their business'. Whether through enhanced cybersecurity, supply chain diversification,

or better risk monitoring, companies need to move from reacting to crises towards anticipating them and investing in mitigation strategies, even when these carry short-term costs.

This is easier said than done, especially for businesses that are accustomed to operating in high-trust commercial environments. Yet many European firms are learning these lessons first-hand. A representative from a company in a critical industry shared a cautionary tale about underestimating the threat from China. The company's sector was identified as one of the 10 strategic sectors China aimed to dominate.[11] In the years that followed, the company's technology was copied, their Chinese factory orders diminished, and Chinese players took over their Chinese market share. As the representative put it, 'we did not strive to become securitised, but we have been securitised'.

At the same time, workshop participants stressed that economic security must not become a pretext for protectionism or excessive interference. While governments can and should nudge businesses to take security more seriously, businesses remain best placed to understand their supply chains and operational needs. Many firms already view economic security as part of their competitiveness agenda, not just a compliance issue. There is growing awareness that strong security practices can be a source of advantage, particularly in a global environment where trust, reliability and resilience are becoming market differentiators.

Public Sector Mindset Shift – from Fragmentation to Coordination

A parallel mindset shift is needed within the public sector – from ministry-specific thinking to whole-of-government approaches that reflect the multidimensional nature of economic security. This is as much a cultural challenge as an administrative one. Integrating economic and security policy perspectives places new demands on public institutions. Decisions once treated as purely economic now require security considerations, and vice versa. This calls for new capabilities within government – teams with both economic literacy and security expertise, and processes that integrate risk insights across departments. Closing these gaps will require a shift in how policymaking is conceived and delivered.

To date, few member states have developed governance structures to coordinate economic security across ministries. Denmark was highlighted by workshop participants as a 'pioneer' in this space, having established an economic security

11. For more information, see Institute for Security & Development Policy, 'Made in China 2025', June 2018, <https://www.isdp.eu/wp-content/uploads/2018/06/Made-in-China-Backgrounder.pdf>, accessed 17 July 2025.

department within its Ministry of Foreign Affairs that is responsible for strategic oversight and coordination across the central administration. Yet even in Denmark, officials acknowledged the difficulty of overcoming ministerial silos, with some departments initially reluctant to engage fully because of fear of unwanted interference in their policy areas.

At the EU level, the need for institutional evolution is even more acute. Many participants stressed the urgency of building stronger governance mechanisms that bridge national and EU-level economic security efforts, while also fostering horizontal coordination across different EU Commission services and European Council bodies. A hybrid approach was proposed that combined cross-cutting policy alignment with technical expertise and regular dialogues between member states, EU institutions and the private sector.

Crucially, this mindset shift must not be purely defensive. The public sector should invest in the 'upside' of economic security – areas where Europe has technological leadership, strategic industrial capacity or the potential to set global standards. Participants called for a holistic EU policy mix that promotes this shift, combining support for competitiveness (through deregulatory efforts and lower energy costs) with the right incentives and frameworks for risk management. As one participant noted, 'staying ahead can be just as important as defending what we have'.

Box 2: Pragmatism in Brief

- **Economic security requires a cultural shift**: Both private and public sectors must adapt long-standing assumptions, practices and operating procedures to reflect today's more contested geopolitical environment.
- **The private sector must integrate security risk into commercial strategy**: Firms need to move from an 'opportunity-first' mindset to one that prioritises geopolitical risk awareness, resilience planning and investment in security.
- **The public sector needs integrated, whole-of-government coordination**: Economic security spans multiple policy domains; siloed governance structures hinder effective risk prioritisation and response.
- **A balance between defensiveness and offensiveness is key**: Economic security policy must not only safeguard vulnerabilities, but also leverage Europe's strengths to lead in innovation, competitiveness and global standard setting.

3. Partnership

The third concept is partnership. If precision provides clarity and pragmatism enables action, then partnership is the connective tissue that brings both to life. At the heart of nearly every observation shared during the Copenhagen workshop (whether on defining risk, shaping responses or shifting mindsets) was the recognition that economic security cannot be delivered by national governments alone.

In Europe's open, market-based economies, the bulk of economic activity occurs in the private sector. Businesses operate infrastructure, build supply chains, invest in critical technologies, and face coercive risks directly. Governments, meanwhile, hold national security responsibilities, legal mandates and secret intelligence. To effectively implement economic security objectives, bringing these capabilities together is not optional, it is essential.

Furthermore, the partnership imperative does not stop at national borders. Deeper collaboration with like-minded countries will be critical to building shared resilience, shaping global standards and ensuring that open economies can thrive in an era of growing strategic competition. These two types of partnerships are explored below.

Government to Business Partnerships

A consistent theme across the Copenhagen workshop was that economic security PPPs must move beyond high-level dialogues into deeper, more formalised collaboration. This sentiment aligns with former UK Deputy National Security Adviser Jonathan Black and others' seminal report on the intersection of security and economic interests, which found that effective policymaking will increasingly demand the sophisticated combining of sovereign intelligence assessment with market insight.[12] As the report states: 'This is necessary to help governments to determine where it is appropriate to intervene in the market for security related reasons, but equally to help businesses price security risk into their commercial decision-making.'[13]

Without business input, governments risk designing economic security policies that miss operational realities or unintentionally distort markets. Without government insight, companies may overlook state-based threats or underestimate geopolitical dynamics. As CFS Senior Associate Fellow, and Taskforce member,

12. Jonathan Black et al., 'The Crossroads of Geopolitics: The Intersection of Security and Economic Interests – Policymaking in a More Complex and Uncertain World', Blavatnik School of Government, Oxford University, p. 45, <https://www.bsg.ox.ac.uk/research/publications/crossroads-geopolitics-intersection-security-and-economic-interests>, accessed 21 July 2025.
13. *Ibid.*

Andrew Cainey observes, '[j]ust as the private sector lacks experience of security matters, so government often lags in understanding the dynamics of multinationals and the global economy'.[14]

To bridge these gaps, Cainey proposes that policymakers need to 'take explicit account of the three dimensions of information, incentives and capabilities – in both government itself and in the private sector'.[15] In practice, this means creating opportunities for the private sector to apply its capabilities, improving secure and reciprocal channels for intelligence-sharing, and aligning incentives so that businesses view economic security as compatible with, rather than contrary to, their commercial goals.

A recurring pattern observed not only in Copenhagen, but also across the Taskforce's broader work, is a misalignment in perceptions – governments often view companies as hesitant to share commercially sensitive risk information, while private sector representatives express a willingness to engage more openly in information exchange.[16] This underscores the need for formal mechanisms that facilitate ongoing, confidential collaboration, not just ad hoc consultation. Structured dialogue and secure intelligence-sharing protocols would help embed economic security in the everyday decision-making of both business and government.

Countries such as Japan, Finland and the UK are actively integrating business into their economic security planning. At a recent CFS workshop, Japanese government representatives explained their extensive legislative and institutional frameworks to increase cooperation between the public and private sectors.[17] Similarly, CFS's engagement with stakeholders from Finland and the UK have highlighted efforts by those countries to formally engage business in economic security planning.[18]

14. Andrew Cainey, 'Economic Security in Practice', Policy Series 2025, No. 9, Lau China Institute, King's College London, p. 9, <https://www.kcl.ac.uk/lci/assets/2025/economic-security-in-practice.pdf>, accessed 22 July 2025.
15. *Ibid.*, p. 4.
16. See Lockhart, 'RUSI European Economic Security Taskforce, Meeting 2', pp. 9–10; BusinessEurope, 'Business Views on a European Economic Security Strategy', Position Paper, May 2024, <https://www.businesseurope.eu/publications/business-views-european-economic-security-strategy-businesseurope-position-paper>, accessed 15 July 2025.
17. For more information, see Shotaro Nagino and Brad Glosserman, 'Japan Sets the Pace for Private Sector Economic Security Management', 1 May 2025, <https://pacforum.org/publications/pacnet-34-japan-sets-the-pace-for-private-sector-economic-security-management/>, accessed 23 July 2025.
18. For more information on Finland, see Tomi Kristeri et al., 'Preparedness for Geoeconomic Risks: Finnish Security in the Age of New Great Power Competition', Finnish Institute of International Affairs, July 2025, <https://fiia.fi/wp-content/uploads/2025/07/RP3_Tomi-et-al_Preparedness-for-geoeconomic-risks.pdf>, accessed 23 July 2025. For more information on the UK, see HM Government, 'Deputy Prime Minister and Business Secretary Join Business Leaders for "First of its Kind" Declassified Economic Security Briefing', 11 December 2023, <https://www.gov.uk/government/news/deputy-prime-minister-and-business-secretary-join-business-leaders-for-first-of-its-kind-declassified-economic-security-briefing>, accessed 23 July 2025.

Lessons can also be drawn from analogous fields. For example, financial information-sharing PPPs have had a significant impact in the fight against economic crime and terrorist financing.[19] These PPPs offer a model for how policymakers, intelligence agencies and businesses can share sensitive data and respond collaboratively to evolving risks. These examples show that with the right governance and protections, information collaboration between sectors is both feasible and highly effective.

Importantly, improved information-sharing can also help the public and private sectors identify where their incentives to strengthen economic security naturally align – and where they do not. As many workshop participants observed, businesses already have strong commercial and economic reasons to reduce foreign dependencies or prevent technological leakage, especially as awareness of geopolitical risks grow. But when economic security priorities impose additional costs or fall outside immediate commercial interests, governments should consider how policy levers such as tax relief and subsidies can reward companies for making security-conscious choices.

Finally, when it comes to aligning incentives, previous Taskforce engagements have highlighted the importance of supporting startups and SMEs, who face disproportionate burdens in navigating economic security risks.[20] SMEs lack the resources available to large multinationals, yet they are often critical nodes in sensitive supply chains. Providing pooled intelligence, tailored guidance and targeted financial support will ensure that the entire business ecosystem, not just its largest players, can engage in productive partnerships with government.

International Partnerships

Economic security is also a shared international challenge. As the EU works to strengthen its internal resilience and deepen relationships with the private sector, it must simultaneously reinforce and expand its partnerships with like-minded third countries. Taskforce members from the private sector often comment that multinational businesses operate across jurisdictions and regulatory systems, therefore coordination among trusted allies – particularly on intelligence-sharing, standard setting and supply chain oversight – is both necessary and mutually beneficial. Closer alignment between Europe and its international partners could reduce friction, improve risk detection, and enhance the overall impact of economic security measures.

19. Nick Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships', *RUSI Occasional Papers* (March 2019), <https://www.rusi.org/explore-our-research/publications/occasional-papers/expanding-capability-financial-information-sharing-partnerships>, accessed 17 July 2025.
20. Lockhart, 'RUSI European Economic Security Taskforce, Meeting 1', p. 7.

Greater international cooperation also enables the EU to take a more strategic, outward-facing role. As participants at the Copenhagen workshop and earlier Taskforce meetings noted, economic security should not be framed solely in defensive terms.[21] The EU can and should leverage its market size and regulatory influence to support the economic resilience of trusted partners through deeper trade ties, financial connectivity and joint investment in critical infrastructure. The recent EU–Japan cooperation on trade and economic security illustrates the value of such partnerships.[22]

These alliances also serve an existential purpose – preserving a free, fair and rules-based global trading system amid rising economic fragmentation. International partnerships can reinforce the integrity of the EU's internal market while resisting the drift towards protectionism. There was general agreement at the Copenhagen workshop that Europe's strength lies not in national champions, but in acting collectively to shape an open, secure and competitive economic order. In this sense, safeguarding Europe's economic security means not only reinforcing its internal foundations but also ensuring that trusted global cooperation continues to thrive.

Box 3: Partnership in Brief

- **Deep public–private collaboration is essential**: Governments must treat businesses as full partners in shaping and implementing economic security policy.
- **PPPs must align information, incentives and capabilities**: Governments need to shape commercial behaviour not just through rules, but also by improving information flows, aligning incentives, and building mutual capacity.
- **Learning from other countries and domains is key**: International models like those in Japan, Finland, and the UK, as well as financial crime intel partnerships, offer valuable lessons in institutional design and information exchange.
- **Strengthening trusted alliances is vital**: Economic security cannot be achieved in a vacuum. Europe must strengthen cohesion within the bloc and collaboration with like-minded countries to promote shared values and build global resilience.

21. Lockhart, 'RUSI European Economic Security Taskforce, Meeting 2', p. 11.
22. European Commission, 'EU and Japan Reaffirm Close Cooperation on Trade and Economic Security', 8 May 2025, <https://policy.trade.ec.europa.eu/news/eu-and-japan-reaffirm-close-cooperation-trade-and-economic-security-2025-05-08_en>, accessed 23 July 2025.

Conclusion

The work of the Taskforce has shown that strengthening Europe's economic security will require more than new policies or a bigger toolbox – it demands a fundamental shift in how both governments and businesses think and operate. The consensus that emerged from the Copenhagen workshop was that three concepts are essential to this transition.

First, precision is key to ensuring that government interventions are targeted, proportionate and risk based. Second, pragmatism involves recognising that economic security cannot be bolted on – businesses must integrate security risks into their commercial operations, while governments must adopt a more cross-cutting approach to policy design and delivery. Third, partnership is the foundation on which any economic security agenda must be built. Domestically, this means deeper collaboration between the public and private sectors to align information, incentives and capabilities. Internationally, it requires working with like-minded countries to strengthen resilience and promote a rules-based order.

In a world of complex economic interdependence, increasingly contested trade relationships, and intensifying geopolitical tensions, Taskforce members viewed this combination of clarity, coherence and collective resolve as offering the most effective path forward.

About the Author

Eliza Lockhart is a Research Fellow at the Centre for Finance and Security at RUSI. Her research examines matters at the intersection of law, finance, and global security. Eliza is a lawyer and legal policy expert with experience advising on economic security, hybrid/state threats, electoral integrity, risk and compliance, and disruptive technologies. Prior to joining RUSI, Eliza worked in Australia for Allens Linklaters and subsequently the Federal Court of Australia as Associate to The Hon. Justice Kenny AM. Eliza holds a Master of Law and an MPhil in Public Policy, both with Distinction, from the University of Cambridge.