



CENTER FOR INTERNATIONAL
PRIVATE ENTERPRISE



economic
security forum

Governing Trusted Supply Chains: Public-Private Coordination in an Era of Geoeconomic Competition

Evidence and Lessons from Australia,
Finland, and South Korea

Prepared for the Center for International Private Enterprise
by the Economic Security Forum (Team: Christian Fjäder,
Marc Ablong, Seungjoo Lee, and Mikael Wigell)

May 2026



About CIPE:

The Center for International Private Enterprise (CIPE) is a global organization that works to strengthen democracy and build competitive markets in many of the world's most challenging environments. Working alongside local partners and tomorrow's leaders, CIPE advances the voice of business in policy making, promotes opportunity, and develops resilient and inclusive economies. Founded in 1983, CIPE is a core institute of the National Endowment for Democracy and an affiliate of the U.S. Chamber of Commerce. CIPE currently has programs in more than 80 countries with private sector and think tank partners.

About the Economic Security Forum:

The Economic Security Forum (ESF) is a geoeconomics advisory and analytics platform focused on the intersection of economic policy, corporate strategy, and national security. ESF works with governments, companies, financial institutions, and international organisations to help decision-makers navigate growing economic fragmentation, strategic competition, and economic security risks.

ESF combines geoeconomic analysis with scenario-based assessment methodologies to support strategic decision-making in areas such as trusted supply chains, strategic competitiveness, technology governance, and resilience. Its work bridges macro-level geopolitical developments with company-level operational and strategic challenges.

Through strategic dialogues, executive programmes, analytical projects, and applied assessment exercises, ESF convenes public and private stakeholders to strengthen resilience, preparedness, and trusted international economic cooperation.

Copyright ©2026 Center for International Private Enterprise (CIPE); all rights reserved

Table of Contents

Executive Summary	1
Chapter 1: The Geoeconomic Turn and Its Implications for Trusted Supply Chains	4
Chapter 2: National Frameworks for Economic Security and Trusted Supply Chains in Australia, Finland, and South Korea	6
2.1 Synthesis of Country Analyses	6
2.2 Australian Government Policies for Economic Security and Trusted Supply Chains.....	9
2.3 Finnish Government Policies for Economic Security and Trusted Supply Chains	29
2.4 South Korean Government Policies for Economic Security and Trusted Supply Chains.....	43
Chapter 3: Corporate Practices, Perceptions, and Constraints in Trusted Supply Chains	53
3.1 Introduction	53
3.2 Survey Scope, Structure, and Respondent Profile	54
3.3 Methodological Caveats.....	55
3.4 Summary of Key Findings	56
3.5 Supply Chain Resilience in Practice	57
3.6 Trusted Supply Chains and International Collaboration	57
3.7 Insights from Open-Ended Responses	58
3.8 Implications for Trusted Supply Chain Policy.....	58
Chapter 4: Case Study Vignettes – Corporate Realities.....	59
4.1 Case Study Vignette 1: The “Fast Follower” Dilemma – Balancing Sovereignty with Commercial Survival in South Korea.....	59
4.2 Case Study Vignette 2: Australian Defense Supply Chain Dynamics – A System-Level Perspective.....	60
4.3 Case Study Vignette 3: Finnish Dual-Use Firms at the Economic Security–Readiness Interface	62
Chapter 5: Governing Trusted Supply Chains – Frictions, Trade-Offs, and Public-private Coordination	66
5.1 Trusted Supply Chains as a Governance Challenge	66
5.2 Visibility as the Persistent Bottleneck.....	67
5.3 The Cost and Distribution of the “Security Premium”	67
5.4 Legal and Regulatory Friction as an Unintended Constraint	68
5.5 Trust, Information, and the Limits of Voluntarism.....	68
5.6 From Friction to Dialogue: Implications for Public-private Coordination.....	69
5.7 Takeaway: Trusted Supply Chains as a Workable Bargain.....	69
Chapter 6: Conclusions and Policy Recommendations.....	70
6.1 From Strategic Alignment to Operational Reality.....	70
6.2 Policy Recommendations.....	71
6.3 Implementation Map: Translating Recommendations into Action.....	73
6.4 Final Takeaway	74
List of Acronyms	75

Executive Summary

The global economy is undergoing a structural transformation in which geopolitical considerations increasingly shape trade, investment, and technology flows. The era in which economic interdependence was assumed to generate political stability has given way to a more contested environment, characterized by strategic competition, selective decoupling, and the active use of economic instruments for security purposes. In this context, trusted supply chains have emerged as a central organizing principle for economic security policy among the United States and its partners.

This report examines how that shift is unfolding in practice, and what it implies for governments and firms operating in strategic and dual-use sectors. Focusing on Australia, Finland, and South Korea, the analysis combines national policy frameworks, a firm-level survey, and targeted case vignettes to explore how trusted supply chains are being constructed – and where implementation frictions persist. These three nations were selected for this report because they represent a cohesive yet geographically diverse sample of countries navigating modern geostrategic risks. Despite their differing histories and locations, Finland, South Korea, and Australia all share a critical focus on **economic resilience** and **supply chain security** in response to global disruptions and economic coercion. By examining these specific nations, the report highlights how "trusted supply chains" and the strengthening of industrial bases, particularly in dual-use technologies like artificial intelligence (AI) and drones, are being operationalized. Ultimately, comparing these three allows for a nuanced analysis of how unique institutional setups and varying relationships with the United States influence national strategies for securing specialized high-tech sectors.

From Globalization to Governed Interdependence

Across all three countries, trusted supply chains are not conceived as a retreat from global markets, nor as a push for comprehensive self-sufficiency. Instead, they represent an effort to govern interdependence more deliberately: reducing exposure to coercion, disruption, and strategic surprise while preserving openness, innovation, and competitiveness.

This shift is particularly pronounced in dual-use technology domains, where civilian innovation and national security are deeply intertwined. Advanced capabilities in artificial intelligence, semiconductors, autonomous systems, advanced sensing, and digital infrastructure are predominantly developed by private firms, yet are increasingly subject to export controls, investment screening, and security-driven regulatory oversight. As a result, companies are no longer peripheral actors in economic security policy; they are central implementers, and increasingly co-governors of trusted supply chains.

National Approaches: Converging Objectives, Diverging Governance Models

The comparative analysis reveals strong convergence in objectives, but significant variation in governance design:

- **Australia** pursues resilience primarily through allied integration, embedding domestic firms into trusted defense and technology supply chains, most notably through mechanisms such as the Global Supply Chain (GSC) Program, AUKUS-

related industrial cooperation, and Security of Supply Arrangements with the United States. The model emphasizes exports, interoperability, and resilience-through-integration rather than sovereign self-sufficiency.

- **Finland** represents a highly institutionalized approach rooted in its Comprehensive Security-model, where preparedness and supply chain resilience are embedded in permanent public-private governance structures. Rather than relying on ad hoc crisis measures, Finland integrates firms into standing security-of-supply institutions that prioritize anticipation, early warning, and trusted interdependence with allies.
- **South Korea** adopts a more state-led and law-driven approach, shaped by direct experiences of economic coercion and supply disruption. Supply chain resilience is pursued through dedicated legislation, centralized coordination (“control tower” governance), early-warning systems, and targeted financial instruments, alongside industrial policy aimed at strengthening upstream capabilities.

Despite these differences, all three countries share a common strategic logic: economic security is no longer separable from national security, and supply chains underpinning critical and dual-use capabilities must be governed accordingly.

The New Corporate Reality: Strategic Alignment, Operational Friction

Survey results¹ and case vignettes show that firms broadly accept the logic of trusted supply chains. Geopolitical risk is now treated as a structural operating condition, not an episodic shock. Companies invest in resilience through technical design choices, contractual arrangements, and diversification strategies.

However, the evidence also reveals a persistent implementation gap between policy ambition and corporate execution:

- Visibility beyond Tier-1 suppliers remains limited across all three countries, even as governments increasingly expect firms to map and manage upstream dependencies.
- Compliance and resilience costs—the “security premium”—are real and unevenly distributed, falling disproportionately on small and medium-sized enterprises (SMEs) that are often critical Tier-2 and Tier-3 suppliers.²
- Legal and regulatory frictions, including competition law, subcontracting rules, data protection regimes, and misaligned export controls, frequently constrain firms’ ability to adjust supply chains in line with security objectives.
- Trust and information-sharing remain fragile. Firms are cautious about sharing sensitive data without clear assurances on liability, reciprocity, and proportionality, while governments struggle to obtain the granular visibility required for effective risk governance.

¹ <https://www.economicsecurityforum.org/publications/nordic-business-snapshot-geo-economic-exposure-and-adjustment-capacity>

² In a supply chain context, **Tier 2** suppliers provide the specific components or processed materials used by direct (Tier 1) suppliers to build major assemblies. **Tier 3** suppliers represent the deeper layer of the chain, typically providing the raw materials or basic commodities—such as minerals or chemicals—required by Tier 2 manufacturers.

The case studies illustrate that trusted supply chains are rarely built on a blank slate. Legacy obligations, installed product bases, long-term service commitments, and deeply embedded industrial ecosystems significantly shape what firms can do, how quickly, and at what cost.

Trusted Supply Chains as a Governance Challenge

Taken together, the findings point to how trusted supply chains are fundamentally a governance problem, not a purely technical, locational, or trade-policy issue. Their durability depends on whether governments and firms can strike a workable governance bargain that aligns security objectives with commercial incentives, clarifies expectations, and distributes costs in a credible and sustainable way.

Where this bargain holds through predictable rules, proportionate obligations, credible information-sharing, and tangible participation value, firms are more likely to internalize economic security objectives as part of core business strategy. Where it breaks down, compliance becomes reactive, trust erodes, and policy effectiveness declines.

The experiences of Australia, Finland, and South Korea demonstrate that there is no single institutional model for achieving this balance. But they also show that success depends less on choosing between markets and states, and more on how public-private coordination is structured, sustained, and operationalized.

Policy Implications

The report concludes with five policy recommendations aimed at closing the gap between strategic intent and operational reality. These focus on:

1. Translating “trusted partner” status from political designation into operational practice;
2. Improving Tier-2 and Tier-3 supply chain visibility without overburdening firms;
3. Addressing the uneven distribution of costs associated with resilience and compliance;
4. Reducing friction from misaligned export controls and compliance regimes among trusted partners; and
5. Treating public-private cooperation as a standing governance system rather than a consultative afterthought or ad-hoc process.

Overall, the findings underscore that trusted supply chains cannot be declared into existence. They must be built, governed, and maintained through structured coordination, credible reciprocity, and sustained dialogue between governments and the private sector. Without such mechanisms, trusted supply chain strategies risk remaining declaratory, strong on intent, but uneven in execution. In an era of intensified geoeconomic competition, the effectiveness of economic security policy will increasingly depend on whether governance arrangements can move decisively from intent to execution.

Chapter 1: The Geoeconomic Turn and Its Implications for Trusted Supply Chains

The international system is undergoing a structural transformation comparable in scale to the post–Second World War and post–Cold War transitions. For roughly three decades, global economic integration was guided by the assumption that openness, efficiency, and market-led allocation would foster political convergence and stability. Supply chains were optimized for cost and speed, capital flowed with limited restriction, and geopolitical risk was largely treated as an external variable rather than a core strategic concern. Economic interdependence was widely viewed as a stabilizing force, while the role of the state in markets receded.

By the mid-2020s, this consensus has eroded. The vision of a unified global marketplace has given way to a more fragmented and contested economic order shaped by **geoeconomics**, i.e. the strategic use of economic instruments, dependencies, and rules to advance national power and security objectives.³ States have re-emerged not merely as market regulators, but as active architects of capital flows, technology development, and industrial capacity. In this environment, commercial decisions are increasingly conditioned by geopolitical alignment, regulatory exposure, and security considerations.

The **Economic Security and Trusted Supply Chains Initiative**, funded by the Center for International Private Enterprise (CIPE) and implemented by the Economic Security Forum, examines how this geoeconomic shift is unfolding among key U.S. allies, and what it means for the organization of secure and reliable supply chains. The project focuses on Finland, Australia, and South Korea as strategically positioned partners with distinct institutional models and critical roles in dual-use technology ecosystems. It combines comparative analysis of national economic security policies with survey-based insights and qualitative case study analysis into how firms assess risk, manage compliance, and make sourcing and partnership decisions under increasing geopolitical constraints. The objective is to **identify best practices and coordination gaps that can be addressed through structured public-private dialogue**.

Several mutually reinforcing dynamics underpin the geoeconomic turn. The COVID-19 pandemic exposed the fragility of highly concentrated production systems and demonstrated the security costs of efficiency-driven optimization.⁴ At the same time, intensifying strategic competition between major powers has reshaped the international economic environment, introducing overlapping and sometimes conflicting trade, technology, and security regimes.⁵ Governments and firms now operate within a landscape where access to markets, technology, and capital is increasingly mediated by strategic considerations.

Within this broader geoeconomic context, **control over critical economic dependencies has become a central source of leverage**. Global networks—including financial infrastructure, digital systems, and advanced manufacturing supply chains—

³ Gillian Tett, 'The New Age of Geoeconomics', *Financial Times*, 12 July 2025.

⁴ Henry Farrell and Abraham L. Newman, 'This is What the Future of Globalization Will Look Like', *Foreign Policy Magazine*, 4 July 2020.

⁵ Milan Babić, Adam Dixon, and Imogen T. Liu, *The Political Economy of Geoeconomics: Europe in a Changing World* (Palgrave Macmillan, 2022).

are characterized by asymmetric concentration around key nodes.⁶ States that exercise influence over these nodes can shape outcomes beyond their borders. As a result, supply chains that were once evaluated primarily on efficiency grounds are now assessed in terms of reliability, resilience, and political exposure.

This shift has elevated the importance of **trusted supply chains** as a practical preparedness strategy in response to geoeconomic risk.⁷ Rather than seeking to disengage from global markets, governments and firms are increasingly focused on ensuring that critical goods, technologies, and services flow through networks—economic corridors—that are transparent, reliable, and aligned with shared legal and security standards. Trust, in this sense, is not ideological but operational. It encompasses confidence in regulatory regimes, protection of intellectual property, data integrity, continuity of supply, and predictable crisis behavior among partners.

These considerations are particularly acute in the domain of **dual-use technologies**, where the boundary between civilian and military innovation has largely collapsed. Advanced capabilities in artificial intelligence, semiconductors, advanced sensing, and autonomous systems are predominantly developed by private firms but carry significant national security implications. Export controls and investment screening regimes have therefore expanded beyond traditional military hardware to include intangible technology transfers such as software, technical data, cloud services, and research and development (R&D) collaboration.⁸ For firms operating in these sectors, compliance has become a strategic constraint shaping investment, partnerships, and long-term competitiveness.

For the middle powers examined in this report, managing dual-use exposure while remaining attractive and reliable partners within trusted supply chains constitutes a central policy challenge. Australia's deepening defense-industrial cooperation with the United States, Finland's integration into North Atlantic Treaty Organization (NATO)-aligned security frameworks, and South Korea's position at the heart of advanced manufacturing all illustrate different approaches to balancing openness with protection. In each case, national policy choices directly shape corporate incentives and capabilities.

As a result, **corporate geoeconomic agency** has become a defining feature of the current economic landscape.⁹ Firms are no longer passive recipients of policy but are active participants in managing economic security outcomes. Governments increasingly rely on private actors to implement sanctions, enforce export controls, and safeguard critical infrastructure, while companies engage in sustained dialogue with public authorities to manage risk, secure exemptions, and shape standards. This convergence has heightened the importance of internal geopolitical competence

⁶ Daniel W. Drezner, Henry Farrell and Abraham L. Newman, *The Uses and Abuses of Weaponized Interdependence* (Brookings Institution Press, 2021).

⁷ Tomi Kristeri, Joel Linnainmäki, Markus Holmgren, and Mikael Wigell, *Preparedness for Geoeconomic Risks: Finnish Security of Supply in an Age of New Great Power Competition*, FIIA Research Paper 3, The Finnish Institute of International Affairs, July 2025.

⁸ Sarah Bauerle Danzman, 'A Tool is Not a Strategy: Technology Security Amidst Contested Global Orders', *Journal of International Economic Law*, Vol 28 (2), 2025, pp. 302-313.

⁹ Henrique Choer Moraes and Mikael Wigell, 'Balancing Dependence: The Quest for Autonomy and the Rise of Corporate Geoeconomics', in Babić et al. (eds.), *The Political Economy of Geoeconomics: Europe in a Changing World* (Palgrave Macmillan, 2022); Victor A. Ferguson, Henrique Choer Moraes, and Mikael Wigell, 'States, Firms, and Geoeconomic Agency: The Role of Private Business in Economic Statecraft and Security', *Law & Geoeconomics*, Vol. 1 (1), 2025, pp. 5-23.

within firms, reflected in the growing attention to board-level oversight of geopolitical and supply chain risk.¹⁰

From a policy perspective, the challenge is not to retreat from globalization, but to **govern interdependence more effectively**. Trusted supply chains offer a framework for doing so by aligning economic efficiency with security requirements, and by clarifying expectations between governments and the private sector. However, trust cannot be declared; it must be operationalized through compatible regulations, information-sharing mechanisms, and credible public-private coordination.

This report is structured as follows. **Chapter 2** provides a comparative analysis of national economic security and trusted supply chain frameworks in Australia, Finland, and South Korea, highlighting how each country approaches resilience, allied integration, and public-private coordination under conditions of geoeconomic competition. **Chapter 3** presents the findings of a firm-level survey conducted across the three countries, examining corporate awareness of geopolitical risk, supply chain resilience practices, and perceptions of government support in dual-use and strategically exposed sectors. **Chapter 4** complements the survey analysis with targeted case study vignettes that illustrate the operational realities, constraints, and trade-offs faced by firms as they navigate economic security requirements in practice. Building on these empirical foundations, **Chapter 5** synthesizes cross-cutting frictions and governance challenges, identifying recurring tensions related to visibility, compliance costs, regulatory alignment, and trust in public-private cooperation. Finally, **Chapter 6** distils the report's core findings into a set of policy-relevant conclusions and actionable recommendations aimed at translating strategic alignment into operationally viable trusted supply chains through improved governance, incentive design, and partner coordination.

Chapter 2: National Frameworks for Economic Security and Trusted Supply Chains in Australia, Finland, and South Korea

This chapter compares the national economic security and supply chain policy frameworks of Australia, Finland and South Korea. The analysis highlights how each country is redefining the relationship between government and business in response to geoeconomic risk—especially in dual-use technology sectors—by building the regulatory, institutional, and partnership foundations for **trusted supply chains**. The central finding is that resilience is no longer only a firm-level risk management question; it has become a governance challenge that requires sustained public-private coordination and practical alignment among U.S. partners.

2.1 Synthesis of Country Analyses

The analyses of Finland, Australia, and South Korea reveal a shared strategic direction: strengthening **economic security** by reducing exposure to disruptive dependencies

¹⁰ Jean-Marc Rickli and Richard Lukacs, The Chief Geopolitical Officer: Guiding Business in a Polarised Era, *Strategic Security Analysis*, Issue 37, Geneva Centre for Security Policy, July 2024.

and by building **trusted supply chains** with reliable partners. Across all three cases, governments have been pushed toward more active supply chain policy by a common set of pressures – pandemic-era disruption, intensifying great power competition, and experiences (direct or anticipated) of economic coercion. The result is a broad shift from viewing supply chains primarily as efficiency systems to treating them as critical infrastructure that must be governed for reliability, continuity, and security.

While the three countries differ substantially in institutional design and policy style, they converge on several core propositions. First, economic security is increasingly treated as inseparable from national security, requiring policies that shape market behavior in strategic sectors rather than merely regulating it. Second, dual-use technologies are at the center of this shift. Artificial intelligence, autonomous systems (including drones), advanced sensors, and enabling technologies (such as semiconductors and cyber infrastructure) are now governed not only as commercial assets but as strategic capabilities that require protection, screening, and controlled collaboration. Third, all three countries seek to reduce risk **without pursuing wholesale disengagement** from global markets. Their dominant approach is diversification and managed exposure—often described as “de-risking”—rather than full decoupling.

Importantly, “trusted supply chains” in these cases are not defined by rhetoric but by operational conditions. Trust is treated as a function of: (i) predictable regulatory regimes and enforceable standards, (ii) protection of intellectual property and sensitive data, (iii) credible crisis behavior among partners (including continuity of delivery), and (iv) alignment in export controls, investment screening, and safeguards around dual-use collaboration. This is where the policy challenge becomes practical: trusted supply chains cannot be created by governments alone, and they cannot be sustained by firms if regulatory uncertainty, compliance burdens, or misaligned incentives undermine competitiveness.

Shared issues across the three country cases

Despite differences in national approach, several shared issues recur across Australia, Finland, and South Korea:

- **Geopolitical drivers and coercion risk:** All three countries link supply chain vulnerability to national security exposure. Disruption events and coercion episodes have elevated the political salience of supply chain policy and accelerated institutional reform.
- **Dual-use governance as the friction point:** Controls on technology, knowledge, and sensitive collaboration have expanded beyond traditional hardware export controls to include intangible transfers (software, data, cloud services, R&D). This creates uncertainty for firms about permissible partnerships, compliance obligations, and the stability of cross-border technology cooperation.
- **Balancing economic exposure and security alignment:** Each country faces a version of the same dilemma: managing significant economic ties with China while deepening security and technology cooperation with the United States and other trusted partners. All three aim to reduce excessive concentration risk while maintaining overall trade openness.

- **Public-private coordination as a capability:** In every case, resilience depends on the quality of public-private cooperation. Governments rely on firms for information, implementation capacity, and innovation; firms rely on governments for predictable rules, targeted support, and credible coordination with allies.

Significant differences in national approach

The differences between the three cases are best understood as differences in **institutional architecture, policy maturity, and how trusted supply chains are operationalized.**

- **Policy foundation and maturity**
 - **Finland** builds on a long-standing, society-wide **Comprehensive Security** model that integrates preparedness and continuity planning through institutionalized public-private structures. Finland's NATO accession has shifted the emphasis from national autonomy toward allied integration in security of supply.
 - **South Korea** has developed a more **event-driven economic security strategy**, shaped by direct experiences of coercion and supply disruptions. Its approach is characterized by formal legal foundations, active industrial policy, and dedicated governance bodies for supply chain stabilization.
 - **Australia** has moved rapidly in response to geopolitical change, but its approach remains more **decentralized and programmatic**, combining targeted industrial policy with defense supply chain integration initiatives, supported by critical infrastructure regulation and resilience coordination bodies.
- **Institutional frameworks and implementation style**
 - **Finland** relies on highly institutionalized public-private coordination and preparedness mechanisms, including structured sectoral "pools" and strategic stockpiling, under central coordinating body the National Emergency Supply Agency (NESA) and its public-private counterpart, the National Emergency Supply Organization (NESO).
 - **South Korea** has built a structured governance system anchored in supply chain laws, a stabilization committee, funding instruments, and early-warning mechanisms to enable faster government-wide response and targeted support.
 - **Australia** emphasizes enabling industry participation in allied defense supply chains through programs and partnerships, alongside critical infrastructure regulation and coordination mechanisms for essential goods.
- **Relationship with the United States and allied integration**
 - All three countries maintain a **Security of Supply Arrangement (SOSA)** with the United States – an intergovernmental framework intended to

facilitate **priority access and mutual support for defense-related goods and services** in peacetime, crisis, and conflict. While implementation modalities differ, SOSA functions as a practical mechanism for anchoring trusted defense-industrial cooperation and clarifying expectations around continuity of supply. In practice, SOSA helps reduce uncertainty about supply assurance and interoperability within allied defense industrial bases, even as export controls and compliance requirements tighten.

- **Finland** is moving toward deeper systemic integration following NATO accession and the Defense Cooperation Agreement (DCA), reshaping how security of supply is planned.
- **South Korea** leverages its strategic role in advanced manufacturing, particularly in semiconductors and batteries, as a basis for alliance cooperation, while managing the domestic political and economic constraints of supply chain reorientation.
- **Australia** operationalizes integration primarily through defense-industrial cooperation, especially AUKUS and defense supply chain embedding mechanisms that elevate Australian firms into trusted nodes in allied production networks.

Overall, the synthesis points to the shared conclusion that trusted supply chains are not primarily a question of “where goods are made,” but of **how security, compliance, and competitiveness are governed across borders**. The decisive challenge is to align government security objectives with corporate operational realities, especially in dual-use sectors, through policy clarity, interoperable rules, and credible public-private coordination mechanisms. This provides the foundation for the report’s later focus on corporate practice (Chapter 3), on implementation frictions (Chapter 4), and on the design of structured dialogue priorities (Chapter 5).

2.2 Australian Government Policies for Economic Security and Trusted Supply Chains

Australia faces a complex and evolving geoeconomic environment in which economic security, supply chain resilience, and defense capability are increasingly interlinked. As a highly open economy with deep integration into global markets, and with significant exposure to strategic competition in the Indo-Pacific, Australia has moved to incorporate security considerations more explicitly into economic and industrial policy. This shift has been accelerated by pandemic-related disruptions, episodes of economic coercion, and growing recognition that supply chains underpinning defense and critical infrastructure require more deliberate governance.

Australia’s approach is shaped by its distinctive strategic position: a close security alliance with the United States, deep economic ties with China, and a growing emphasis on regional engagement in the Indo-Pacific. Starting from a relatively low industrial base in certain defense and advanced manufacturing domains, the effectiveness of recent reforms will take time to fully materialize. Nevertheless, the policy direction is clear. Economic security is now treated as a whole-of-government

and whole-of-economy challenge, requiring sustained public-private cooperation and alignment with allied frameworks for trusted supply chains.

2.2.1 Economic and Supply Chain Resilience Policies

Australia recognizes that reliance on a limited number of suppliers, particularly in sectors critical to national security, critical infrastructure, and advanced manufacturing, poses significant economic and strategic risks. The COVID-19 pandemic, combined with episodes of economic coercion and rising geopolitical tensions in the Indo-Pacific, underscored the vulnerability of highly concentrated global supply chains. In response, successive Australian governments have emphasized the need to build more resilient, transparent, and diversified supply chains as a core component of economic security.

While Australian policy does not consistently employ the language of “friendshoring,” many of its initiatives implicitly prioritize the development of **trusted supply chains** with reliable partners. The emphasis is on reducing exposure to high-risk dependencies, improving visibility across supply networks, and ensuring continuity of supply for essential goods and technologies, rather than pursuing wholesale disengagement from global markets. This approach reflects a pragmatic effort to balance economic openness with security imperatives.

Australia’s **National Interest Framework** represents a key evolution in this direction, integrating security considerations more explicitly into domestic economic policymaking. The framework guides decisions related to trade, investment, and supply chains by weighing economic efficiency against resilience, national security, and long-term strategic risk. In practice, this has meant a greater willingness to diversify away from narrow comparative-advantage logics and to favor partnerships with countries that offer regulatory predictability, political reliability, and shared security interests.

A central pillar of Australia’s economic resilience strategy is the strengthening of domestic industrial capability in areas considered critical to national security and economic continuity. The **National Reconstruction Fund (NRF)** plays an important role in this regard, supporting investment across the manufacturing value chain, including sectors linked to critical minerals, clean energy technologies, and defense-relevant capabilities.¹¹ While not framed exclusively as a supply chain security instrument, the NRF contributes directly to reducing vulnerabilities by expanding domestic capacity and supporting more resilient production ecosystems.

Australia also seeks to leverage its comparative advantages in **critical minerals** to position itself as a reliable supplier within trusted international supply chains. Rather than remaining solely an exporter of raw materials, policy initiatives increasingly emphasize downstream processing and value-added manufacturing, particularly in cooperation with strategic partners. This reflects a broader objective of embedding Australia more deeply into allied production networks while reducing exposure to upstream supply risks.

At the same time, Australian policymakers are acutely aware of the costs associated with enhancing supply chain resilience. Diversification, redundancy, and higher

¹¹ Department of Industry, Science and Resources. (2022). *National Reconstruction Fund: Diversifying and transforming Australia’s industry and economy*. Australian Government. <https://www.industry.gov.au/news/national-reconstruction-fund-diversifying-and-transforming-australias-industry-and-economy>

standards of security and compliance can increase costs for both government and industry. As a result, the government has stated its intention to focus resources strategically on areas where risks and potential impacts are greatest, rather than attempting to restructure supply chains wholesale.

Australia's approach is further shaped by the need to manage its complex economic relationship with China, which remains its largest trading partner, driven largely by Australian exports of raw materials, energy, and other industrial inputs, alongside its close strategic alliance with the United States. Rather than framing policy in terms of decoupling, Australian governments have consistently emphasized **de-risking**, seeking to reduce excessive dependence on any single market while expanding trade and investment with a broader range of partners. This strategy is often described by policymakers as "selling more to new partners" rather than trading less with existing ones.¹²

Within this balancing act, trusted supply chains function as a practical organizing principle. By improving resilience, diversifying sources, and deepening cooperation with reliable partners, Australia aims to reduce strategic exposure while preserving the benefits of global economic integration. The effectiveness of this approach will depend not only on policy design but also on sustained public-private cooperation and the willingness of firms to adapt business models in line with evolving economic security objectives.

Policy Towards the United States

Australia places a consistently high priority on its alliance with the United States, viewing it as central to national security, defense planning, and long-term strategic stability. This alliance also plays a critical role in Australia's approach to economic security, particularly in sectors where supply chain resilience and defense capability intersect. Alignment with U.S. policy frameworks and industrial ecosystems is therefore a core element of Australia's efforts to strengthen trusted supply chains in strategic and dual-use domains.

Economic security cooperation with the United States is especially prominent in areas such as critical minerals, advanced manufacturing, and defense-related technologies. Australia has expressed a strong willingness to deepen economic and industrial ties with the United States through comprehensive cooperation arrangements that support secure access to inputs essential for advanced technologies and defense systems.¹³ These efforts reflect converging interests in reducing exposure to supply chain disruptions and in ensuring that critical materials and components are sourced from reliable partners operating under compatible regulatory and security standards.

Australia's approach emphasizes integration rather than insulation. By embedding Australian firms more deeply into U.S.-linked production and innovation networks, policymakers aim to enhance both national resilience and alliance interoperability. This strategy is evident in Australia's participation in U.S.-led initiatives to strengthen supply

¹² Farrell, D. (2025, July 25). *Navigating Australia's trading future* [Speech transcript]. Minister for Trade and Tourism, Australian Government. <https://www.trademinister.gov.au/minister/don-farrell/speech/lowy-institute-keynote-speech-navigating-australias-trading-future>

¹³ Wroe, D. (2025, July 24). *With China visit, Australia signals its own agency to US*. The Strategist. <https://www.aspistrategist.org.au/with-china-visit-australia-signals-its-own-agency-to-us/>

chains for technologies vital to defense, clean energy, and advanced industry, where predictability of supply and regulatory alignment are increasingly valued alongside cost and efficiency.

At the same time, Australian policymakers remain attentive to the need for flexibility and national autonomy within the alliance framework. While alignment with U.S. economic security priorities is strong, Australia seeks to ensure that cooperation enhances domestic capability and does not simply displace risk or concentrate dependence elsewhere. This has informed Australia's emphasis on developing sovereign industrial capacity in selected areas, while leveraging U.S. partnerships to complement, rather than substitute for, domestic capability.

Overall, Australia's policy toward the United States reflects a pragmatic understanding of alliance-based economic security. Trusted supply chains are not viewed as static or exclusive arrangements, but as evolving networks that require continual coordination, transparency, and mutual assurance. The effectiveness of this approach depends on sustained policy alignment, credible security commitments, and the capacity of firms on both sides to operate within increasingly complex regulatory and compliance environments.

Policy Towards China

Australia's approach to China is characterized by calibrated engagement aimed at stabilizing bilateral relations while safeguarding core national interests and economic security. China remains Australia's largest trading partner, and the Australian government continues to recognize the economic importance of maintaining functional commercial ties. At the same time, experiences of economic coercion and broader geopolitical competition have reinforced the need to reduce strategic vulnerabilities and strengthen resilience in critical supply chains.

Following a period of heightened bilateral tension, high-level political and diplomatic engagement has resumed. This includes ministerial dialogues and leader-level visits, with the stated objective of stabilizing relations and restoring predictable trade conditions. Efforts at trade normalization have focused on the removal of tariffs and informal barriers affecting Australian exports such as barley, wine, and coal. These steps reflect a pragmatic recognition that economic disengagement from China is neither feasible nor desirable for Australia's overall economic interests.

Selective engagement with China continues in areas of mutual interest, including climate change, agriculture, education, and people-to-people exchanges. These domains are viewed as lower-risk and conducive to confidence building, even amid strategic competition. At the same time, Australia remains cautious about cooperation in sensitive sectors involving critical infrastructure, advanced technologies, or defense-related capabilities, where national security considerations predominate.

Australian officials consistently stress that China policy decisions are based on Australia's national interests and sovereign assessments rather than external pressure.¹⁴ This framing underscores a desire to preserve strategic autonomy while remaining closely aligned with key security partners. In practice, this means maintaining

¹⁴ Collinson, E. (2025). An independent China policy suited to the times. Asialink. <https://asialink.unimelb.edu.au/diplomacy/independent-china-policy-suited-times/>.

economic engagement where risks are manageable, while actively reducing exposure in areas where dependencies could be exploited for coercive leverage.

Within this framework, China is neither treated as a comprehensive strategic adversary nor as a purely commercial partner. Instead, Australia's China policy reflects a compartmentalized approach: stabilizing trade where possible, limiting exposure in critical sectors, and embedding long-term resilience through diversification and trusted supply chain cooperation with like-minded partners. This balancing act is central to Australia's broader economic security strategy and shapes its evolving approach to supply chain resilience in an era of heightened geopolitical uncertainty.

2.2.2 Evolving Economic Policy Frameworks

Australia's evolving economic policy frameworks reflect a growing recognition that economic resilience and national security are increasingly interconnected. In response to supply chain disruptions, geopolitical competition, and experiences of economic coercion, the Australian government has progressively integrated security considerations into its economic policymaking. At the same time, it has sought to preserve Australia's long-standing commitment to open markets, foreign investment, and a rules-based international economic order.

Rather than constituting a single, centralized "economic security doctrine," Australia's approach is best understood as a layered governance architecture. This architecture combines targeted industrial policy, risk-based regulation, and international economic engagement to manage strategic vulnerabilities without resorting to broad protectionism or economic isolation.

Core Economic Security and Industrial Policy Frameworks

At the center of Australia's current approach is the **Future Made in Australia** policy agenda,¹⁵ which serves as the cornerstone of the government's economic security strategy. Its primary objective is to strengthen domestic manufacturing and processing capabilities in sectors considered critical for long-term economic resilience, national security, and the net-zero transition.

Key components of this framework include:

Targeted Investment, with a focus on:

- refining and processing critical minerals;
- producing renewable hydrogen;
- developing low-carbon liquid fuels and green metals; and
- supporting clean energy technology manufacturing.

Five Tests for Investment, which guide decisions on government intervention:

1. Competitiveness and productivity;
2. Contribution to an orderly path to net zero;
3. Building capabilities of people and regions;

¹⁵ The Treasury. (2024). *Future Made in Australia*. Australian Government. <https://treasury.gov.au/policy-topics/future-made-australia>

4. Improving national security and economic resilience, operationalized through the **National Interest Stream**;
 5. Delivering value for money while recognizing the central role of the private sector.
- **National Interest Stream**, designed to address critical risks where domestic sovereign capability is deemed necessary to protect national security or ensure economic resilience.
Front Door for Investors, intended to streamline approvals for low-risk foreign investments and attract essential capital, while maintaining safeguards for sensitive sectors.¹⁶

Together, these elements illustrate Australia's preference for **disciplined, criteria-based intervention**, aimed at correcting strategic vulnerabilities rather than reshaping the economy wholesale.

Complementing this agenda is the **National Interest Framework**, which explicitly integrates security considerations into economic decision-making related to trade, investment, and supply chains. The framework does not displace growth objectives but adds a systematic assessment of dependency, concentration risk, and exposure to external shocks.

Infrastructure, Supply Chains, and Critical Inputs

Australia has also strengthened its regulatory and institutional foundations for supply chain and infrastructure resilience. A central pillar of this effort is the expansion of the **Security of Critical Infrastructure Act (SOCl)**,¹⁷ which has broadened coverage across 11 critical sectors and introduced enhanced obligations related to risk management, cybersecurity, and supply chain security. These reforms are intended to improve government visibility over systemic vulnerabilities and ensure that essential assets are better protected against both physical and cyber threats.

To support coordination and early identification of risks, the government has established the **Office of Supply Chain Resilience (OSCR) in July 2021**.¹⁸ It functions as a central advisory and coordination body responsible for identifying vulnerabilities in essential supply chains and advising government on targeted interventions. Unlike stockpiling-based models, OSCR operates through risk triage, market intelligence, and transparency rather than direct state control of inventories. Importantly, OSCR acts as a boundary manager rather than a command authority, linking civilian supply chain risk awareness with national security priorities without formally securitizing the broader economy. Its role is to surface systemic dependencies, tier-2 and tier-3 vulnerabilities, and potential points of external leverage, allowing policy responses to be calibrated across economic, infrastructure, and defense domains. In this sense, OSCR functions as a signal generator rather than an executor, providing early warning and coordination inputs that inform sectoral policies, regulatory oversight, and defense planning, while leaving implementation largely to markets, line ministries, and private actors.

¹⁶ The Treasury. (2024). *Future Made in Australia*. Australian Government. <https://treasury.gov.au/policy-topics/future-made-australia>

¹⁷ *Security of Critical Infrastructure Act 2018* (Cth). <https://www.legislation.gov.au/C2018A00029/latest/text>

¹⁸ Department of Industry, Science and Resources. (n.d.). *Office of Supply Chain Resilience*. Australian Government. <https://www.industry.gov.au/trade/office-supply-chain-resilience>

The **Critical Minerals Strategy**, including plans for a future strategic reserve, further reflects Australia's effort to address upstream vulnerabilities. The strategy aims not only to secure access to critical inputs but also to position Australia as a processor and value-adding participant in trusted international supply chains, rather than solely a raw-material exporter.¹⁹

Diversification, Productivity, and External Economic Engagement

A defining feature of Australia's economic security approach is its continued outward orientation. The **economic diversification imperative**, shaped by past trade disruptions, emphasizes reducing market concentration risk by expanding trade and investment relationships rather than disengaging from existing partners. This strategy is framed as "selling more to new partners," not withdrawing from established markets.²⁰

Australia's commitment to multilateralism remains a central stabilizing force. Active engagement in forums such as the **United Nations, World Trade Organization, G20, and the Asia-Pacific Economic Cooperation**, alongside participation in trade agreements including the **Comprehensive and Progressive Agreement for Trans-Pacific Partnership** and the **Regional Comprehensive Economic Partnership**, reflects an effort to anchor economic security policies within a rules-based international system.

This external orientation is reinforced through targeted regional and bilateral initiatives, including:

- the **Southeast Asia Economic Strategy to 2040**, supported by a AUD 505.9 million government commitment and a Southeast Asia Investment Financing Facility of up to AUD 2 billion;
- the **Australia–India Business Exchange**, aimed at leveraging the Australia–India Economic Cooperation and Trade Agreement to unlock new commercial opportunities;
- ongoing **foreign investment review reforms**, intended to deliver a faster, more transparent, and more predictable investment framework.

Finally, senior policymakers continue to situate economic security within a broader **productivity and economic reform agenda**. Government messaging consistently stresses that resilience must be accompanied by competitiveness and productivity growth, acknowledging that long-term economic strength underpins national security.

Taken together, these evolving economic policy frameworks demonstrate Australia's effort to recalibrate its economic model for a more contested global environment. The approach seeks to strengthen resilience through selective intervention, improved risk governance, and diversification, while maintaining openness, private-sector leadership, and deep integration into the global economy. This balance provides the policy

¹⁹ Albanese, A. (2025, April 24). *Albanese Government to establish critical minerals strategic reserve* [Media release]. <https://anthonyalbanese.com.au/media-centre/albanese-government-to-establish-critical-minerals-strategic-reserve>

²⁰ Wong, P. (2024, April 17). *Securing Australia's future in the world* [Media release]. Minister for Foreign Affairs, Australian Government. <https://www.foreignminister.gov.au/minister/penny-wong/media-release/securing-australias-future-world>

foundation upon which Australia's defense supply chain resilience and trusted international partnerships are subsequently built.

2.2.3 Defense Supply Chain Resilience Policies

Australia increasingly views defense supply chain resilience as a core pillar of national security in an era of intensified great power competition and persistent supply chain disruption. The government's approach reflects the assessment that reliance on globally optimized, just-in-time defense supply chains exposes Australia to unacceptable operational risk during crises or conflict, particularly given its geographic distance from major allies and its dependence on imported defense materiel and components.

Strategic Rationale and Policy Foundations

The strategic rationale for strengthening defense supply chain resilience is articulated most clearly in the **2023 Defense Strategic Review** and the **2024 National Defense Strategy**.²¹ These documents emphasize that Australia must be able to sustain military operations in a more contested Indo-Pacific environment, including under conditions of supply disruption or delayed allied support. As a result, resilience, redundancy, and assured access to critical inputs are treated as strategic requirements rather than efficiency considerations.

These priorities are further operationalized in the **Defense Industry Development Strategy (DIDS)**, released in early 2024. The DIDS reframes defense industry policy around the concept of an "integrated force," linking operational requirements, industrial capability, and allied interoperability.²² A central premise of the strategy is that a resilient defense industrial base depends not only on domestic production, but also on sustained export activity and integration into allied supply chains. Exports are therefore treated not as a secondary benefit, but as a necessary condition for industrial viability and readiness.

Building Domestic Capability and Reducing Vulnerabilities

Australia has increased investment in domestic manufacturing, sustainment, and maintenance capabilities to reduce reliance on vulnerable external sources. While not exclusively defense-focused, the **NRF** plays a complementary role by supporting manufacturing capability across the value chain, including sectors with direct relevance to defense supply resilience.²³

The **Critical Minerals Strategy** also underpins defense resilience efforts. Australia's significant reserves of lithium, rare earths, and other critical inputs are increasingly framed as strategic assets for defense technologies, including advanced sensors, communications systems, and guided weapons. Policy efforts aim to ensure that these

²¹ Australian Department of Defence. 2024. *National Defence Strategy*. Commonwealth of Australia. p.18. <https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program>.

²² Australian Department of Defence. 2024. *Defense Industry Development Strategy*. Commonwealth of Australia. Chapter 9. <https://www.defence.gov.au/about/strategic-planning/defence-industry-development-strategy>.

²³ Husic MP, The Hon Ed, Minister for Industry and Science. "Backing regional industry and delivering secure jobs of the future". Media Release, 25 October 2022. <https://www.minister.industry.gov.au/ministers/husic/media-releases/backing-regional-industry-and-delivering-secure-jobs-future>

materials can be processed domestically or within trusted partner networks, reducing exposure to supply disruptions or external pressure.²⁴

Allied Integration and Trusted Defense Supply Chains

Australia's defense supply chain strategy is explicitly anchored in allied integration, particularly with the United States. While Australia does not use "friendshoring" as a formal policy term, the logic of trusted supply chain integration is deeply embedded in its defense posture.

Australia's status as a **SOSA** partner with the United States is a foundational element of its defense supply chain resilience and broader economic security framework. The SOSA provides a formal, though non-binding, mechanism for mutual priority access to defense-related goods and services during peacetime, crisis, and armed conflict.²⁵ Under this arrangement, the U.S. Department of Defense can request priority delivery from Australian suppliers, while Australia's defense organization can obtain reciprocal priority support from U.S. firms.

This mutual assurance of supply constitutes a critical layer of protection against disruptions in defense materiel and industrial inputs. Rather than pursuing full self-sufficiency, the SOSA institutionalizes **trusted interdependence**, aligning with Australia's broader economic security objective of de-risking dependence by securing access to critical capabilities through reliable partners. It allows Australia to leverage allied industrial depth while maintaining productive, market-based supply chains.

Beyond supply assurance, the SOSA promotes interoperability by encouraging reciprocal acquisition of defense goods and closer alignment of industrial standards. This strengthens joint operational planning and facilitates integration between the Australian Defense Force and U.S. forces. The arrangement also enhances opportunities for Australian firms to participate in the U.S. defense industrial base, gaining access to advanced technologies, production methods, and long-term export markets.

The SOSA operates in concert with complementary frameworks such as the **Defense Trade Cooperation Treaty (DTCT)**,²⁶ which enables license-free export of certain defense articles between Australia and the United States. Together, these mechanisms reduce administrative friction, streamline procurement processes, and support efficient collaboration on joint projects and exercises. They also underpin deeper capability development under **AUKUS**, including advanced technologies under Pillar Two and highly sensitive cooperation under Pillar One, such as the nuclear-powered submarine program.

Taken together, the SOSA illustrates how Australia anchors its defense supply chains within a trusted allied ecosystem. It provides a practical example of how economic security objectives—resilience, interoperability, and assured access—can be achieved

²⁴ Australian Department of Industry, Science and Resources. 2023. Critical Minerals Strategy 2023–2030. Commonwealth of Australia. <https://www.industry.gov.au/publications/critical-minerals-strategy-2023-2030>

²⁵ The Treaty was implemented in Australia through the *Defence Trade Control Act 2012*. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r4700#:~:text=Summary,creates%20offences%20and%20imposes%20penalties

²⁶ Corben, Tom & Mayo, Sophie. 2025. "Federation is deterrence: The US defence industrial and technology integration agenda in the Indo-Pacific". United States Studies Centre. Accessed on 24 July 2025. <https://www.ussc.edu.au/federation-is-deterrence-the-us-defence-industrial-and-technology-integration-agenda-in-the-indo-pacific>

through structured public-private and international cooperation rather than through inward-looking industrial protection.

Australia's participation in **AUKUS** further deepens this integration. While **Pillar I** focuses on conventionally armed, nuclear-powered submarines, **Pillar II** is particularly relevant to defense supply chain resilience. It facilitates joint development and production of advanced capabilities in areas such as cyber, artificial intelligence, quantum technologies, undersea systems, and autonomous platforms. These initiatives aim to create an integrated defense innovation and production ecosystem among Australia, the United Kingdom, and the United States, reducing duplication and strengthening trusted industrial linkages.

Australia's **AUD 3 billion investment in U.S. shipyards** to expand submarine production capacity illustrates the depth of this integration. Rather than pursuing full sovereign production, Australia is investing in allied capacity to ensure reliable access within a trusted framework.

Regulatory Alignment and Trade Facilitation

Defense supply chain resilience is also supported through regulatory reform. Amendments to the **Defense Trade Controls Act**, including the **Defense Trade Controls Amendment Act 2024**, aim to better align Australia's export control regime with those of the United States and the United Kingdom. This alignment is intended to reduce friction in defense trade, facilitate technology sharing, and streamline collaboration within trusted partner frameworks.

Complementary arrangements, such as the **DTCT** with the United States, allow for license-free export of certain defense articles between the two countries. These mechanisms reduce administrative burden while preserving safeguards for sensitive technologies, supporting more resilient and predictable defense supply chains.

Data, Risk Assessment, and Emerging Challenges

Australian authorities increasingly recognize that traditional supply chain risk management tools are insufficient in a contested strategic environment. Defense supply chain resilience efforts are therefore expanding to include enhanced data collection, risk mapping, and vulnerability assessment, including at lower tiers of the supply chain.

This shift reflects an understanding that defense supply chains are only as resilient as their weakest nodes, many of which lie outside prime contractors and are often embedded in civilian industrial ecosystems. Addressing these vulnerabilities remains an ongoing challenge, particularly for small and medium-sized enterprises that face compliance, cybersecurity, and financing constraints.

Table 1: The Principal Elements of Australian Economic Security Approach

Strategic Policy and Coordination	Defense Innovation & Capability	Market Access and Export Integration
National Defense Strategy	ASCA	GSC Program
Defense Industry Development Strategy (DIDS)	GWEO	DFAT/Austrade supply chain resilience initiatives (e.g. Supply Chain Resilience Initiative with India and Japan).
Office of Supply Chain Resilience (OSCR)	State-level defense strategies DISP/Cyber uplift	

2.2.4 The Role and Impact of the Global Supply Chain (GSC) Program

The **GSC Program, established in 2007**, is a central instrument in Australia’s approach to defense supply chain resilience and international industrial integration. Rather than focusing solely on domestic procurement or local content requirements, the GSC Program is explicitly designed to embed Australian firms, particularly SMEs, into the global supply chains of major allied defense prime contractors. In doing so, it strengthens sovereign industrial capability while reinforcing trusted international production networks.

Objectives and Design

The GSC Program is funded by the Australian Department of Defense and operates on the premise that long-term resilience of the defense industrial base depends on sustained participation in global markets. Domestic demand alone is insufficient to support scale, continuous production, and skills retention across the defense sector. By enabling Australian firms to access export opportunities, the program aims to smooth demand volatility, enhance competitiveness, and ensure that critical capabilities remain viable over time.

Under the program, selected global defense primes referred to as “GSC Partners” establish dedicated teams responsible for identifying suitable Australian suppliers and integrating them into their international supply chains. These primes actively advocate for Australian firms within their global networks, helping them navigate qualification requirements, compliance standards, and contracting processes. Participation is competitive and merit-based; Australian companies must meet stringent quality, cost, security, and delivery requirements to secure contracts.

Embedding Australian Firms in Trusted Supply Chains

A distinguishing feature of the GSC Program is that it moves beyond traditional offset arrangements or one-off local content obligations. Instead, it seeks to create enduring production relationships in which Australian firms become trusted, repeat suppliers for global defense programs. Once embedded, these firms are less exposed to fluctuations in domestic procurement cycles and more closely integrated into allied defense ecosystems.

From an economic security perspective, this model transforms Australian SMEs from peripheral subcontractors into strategic nodes within trusted supply chains. It strengthens interoperability, improves visibility across lower-tier suppliers, and

enhances resilience by diversifying production locations across allied partners rather than concentrating risk in a single jurisdiction.

Scale and Impact

The impact of the GSC Program has been significant. As of mid-2024, the program had facilitated contracts worth more than **AUD 2.35 billion** to over **300 Australian suppliers**. The Albanese government has expanded the program by nearly doubling the number of participating primes, increasing opportunities for Australian firms to access international defense markets.

Participating primes include major global defense contractors such as **BAE Systems, Boeing, Lockheed Martin, Raytheon, Rheinmetall, Thales, and Babcock**, among others. This expansion has broadened the program's reach across multiple domains, including aerospace, maritime sustainment, land systems, guided weapons, and advanced technologies.²⁷

The program's performance framework has evolved to place greater emphasis on scaling supplier capabilities, early identification of innovation opportunities, and strengthening the pipeline between domestic and international projects. Industry engagement initiatives such as "Pitch to the Primes" events support supplier development and facilitate direct interaction between Australian firms and global defense integrators.

Strategic Significance

From a policy perspective, the GSC Program operationalizes Australia's preference for resilience through integration rather than self-sufficiency. By anchoring Australian industry within allied production networks, the program reinforces mutual dependence with trusted partners while reducing exposure to untrusted or potentially coercive supply relationships.

The program also complements Australia's broader defense and economic security frameworks, including the Defense Industry Development Strategy and the Security of Supply Arrangement with the United States. Together, these mechanisms ensure that Australian firms are not only capable suppliers in peacetime but are positioned to support allied defense needs under conditions of stress or disruption.

Limitations and Challenges

Despite its success, the GSC Program faces challenges. Participation requires significant upfront investment by SMEs in compliance, cybersecurity, quality assurance, and export controls. Smaller firms may struggle to meet these requirements without sustained support. In addition, while the program enhances integration at Tier 1 and Tier 2 levels, visibility and resilience further down the supply chain remain limited.

²⁷ McLaughlin, Andrew. 2024. "Government expands defence industry Global Supply Chain Program". [psnews.com.au](https://psnews.com.au/government-expands-defence-industry-global-supply-chain-program/139261/). Accessed on 24 July 2025. <https://psnews.com.au/government-expands-defence-industry-global-supply-chain-program/139261/>.

Nevertheless, the GSC Program stands out as a practical example of how governments can leverage public-private cooperation to strengthen trusted supply chains, enhance industrial resilience, and align commercial incentives with national security objectives.

Australia's Global Supply Chain Program as a Trusted Supply Chain Enabler

Since its inception, Australia's GSC Program has evolved into a key mechanism for exporting sovereign industrial capability into the global platforms of major defence primes. By October 2025, the program had facilitated more than \$2.35 billion in contracts to over 307 Australian suppliers, with annual contract values growing by nearly 30 per cent in the previous 12 months alone. Officials have told parliamentary committees that this represents a return on investment of roughly 12:1 since 2007, with more than 2,000 contracts worth over \$1.6 billion to around 230 suppliers recorded in earlier years, illustrating the compounding effect as additional primes have been added to the program. For members of the Joint Standing Committee on Foreign Affairs, Defense and Trade (JSCFADT), this has underlined that the key to sustaining a viable defense industry is not "making whole platforms" but securing a durable place for Australian firms in complex global supply chains.

Boeing's long running participation demonstrates how the model works in practice. Since joining the program in 2007, Boeing has generated more than 1,700 bid opportunities for Australian companies, resulting in close to \$1 billion in export contracts across roughly 70-105 suppliers, supporting both commercial and defense programs. Defense witnesses to Parliamentary Committees have explained that these contracts are won on merit rather than through traditional offsets, echoing earlier committee findings on programs such as the Joint Strike Fighter: Australian businesses must compete on cost, quality and schedule to win work, but once they do, they plug into long term global production runs. In evidence, officials have pointed to precision engineered components like Joint Direct Attack Munition-Extended Range wing kits and helicopter structures, as well as software and sustainment services, as examples of areas where Australian SMEs have built globally competitive niches under the GSC framework.

Newer primes such as Babcock illustrate the program's expansion into maritime sustainment and services. Selected as a GSC partner in 2024, Babcock established a dedicated GSC delivery team in Australia and the United Kingdom to identify and qualify local suppliers across marine, aviation, mission systems, nuclear and land domains. Within months, it had secured its first tranche of GSC contracts, awarding work to multiple Australian SMEs for maintenance and support on allied naval platforms and using major international trade shows to showcase those companies to other parts of its global business. In answers to JSCFADT questions about how such arrangements help smaller firms move beyond one off domestic projects, Defense has highlighted the GSC model as "absolutely critical" to the success of SMEs that might otherwise be shut out of large, prime dominated panels, by providing an export pipeline and smoothing volatility in local demand.

Committee members have also pressed Defense on whether the benefits of the GSC Program are sufficiently spread across regions and tiers of industry, and how it interacts with other tools such as the Australian Industry Capability and Defense Industry Development Strategy. Officials have responded that the GSC Program is one of several levers used to "open up opportunities for Australian companies", particularly SMEs, by driving primes to identify new suppliers, mentor them through quality, cyber and export compliance upgrades, and then embed them into international work packages rather than treating local content purely as a domestic obligation. For firms, this lowers entry barriers into complex allied supply chains; for government, it converts industry policy and committee driven expectations into durable, trusted production relationships within allied defense supply chains.

2.2.5 Public-private Cooperation in Australian National Defense and Security

Australia's approach to defense and economic security is underpinned by an extensive system of public-private cooperation that reflects both necessity and design. The government recognizes that it does not possess, on its own, the industrial capacity, technological depth, or innovation speed required to respond to contemporary security challenges. As a result, the traditional "buyer-supplier" relationship between the state and defense industry has progressively evolved into a more integrated **strategic partnership model**, in which private firms are treated as essential contributors to national resilience.²⁸

This shift has been driven by three interrelated pressures: the accelerating pace of technological change, the blurring of civilian and military innovation, and the increasing fragility of global supply chains. Together, these dynamics have forced Australian policymakers to rethink how industry is mobilized, incentivized, and governed in support of national defense objectives.

From Procurement to Strategic Partnership

Historically, Australia's defense industry policy centered on procurement efficiency and project delivery. In the current environment, however, defense policy increasingly emphasizes **industrial readiness, innovation capacity, and sustained participation in allied supply chains**. This has led to a more interventionist, but still market-mediated, approach, in which the state actively shapes incentives while relying on private firms to deliver capability.

The **DIDS** provides the overarching framework for this transition. Released in 2024, the DIDS consolidates previously fragmented industry policies into a single strategic blueprint aligned with the concept of an "Integrated Force." It identifies priority industrial capabilities, promotes exports as a source of resilience, and explicitly links defense industrial policy to supply chain security and allied interoperability.²⁹

Within the DIDS, **Sovereign Defense Industrial Priorities (SDIPs)** define areas where Australia must maintain domestic capability to ensure freedom of action during crises. These priorities do not imply full self-sufficiency, but rather targeted capability retention within a broader ecosystem of trusted international partners³⁰.

Driving Innovation: The ASCA Model

A central pillar of Australia's public-private cooperation model is the **Advanced Strategic Capabilities Accelerator (ASCA)**, which became operational in July 2023. ASCA was established to address a persistent structural challenge: the failure of promising defense-related research and innovation to transition rapidly into deployable military capability.³¹

²⁸ Department of Defence (2023). Defence Strategic Review 2023. Commonwealth of Australia. <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>. Accessed 30 December 2025

²⁹ Department of Defence (2024a). Defence Industry Development Strategy (DIDS). Commonwealth of Australia. <https://www.defence.gov.au/about/strategic-planning/defence-industry-development-strategy>. Accessed 30 December 2025.

²⁹ Department of Defence, 2024a

³⁰ Department of Defence, 2024a

³¹ Department of Defence, 2023

With a budget of AUD 3.4 billion over ten years, ASCA operates as a **capability accelerator** rather than a traditional grant body. Located within the Vice Chief of the Defense Force Group and linked to the Capability Acquisition and Sustainment Group, ASCA is designed to shorten acquisition timelines and align innovation directly with operational needs.

Crucially, ASCA changes the risk calculus for private firms. Regulatory reforms allow companies to retain intellectual property generated through joint projects and introduce “honorable failure” provisions that reduce penalties for unsuccessful high-risk research. This approach treats defense innovation more like venture capital than conventional procurement, encouraging firms to pursue asymmetric and dual-use technologies without existential financial risk.

Strategic Implications: ASCA and DIDS

- **Advanced Strategic Capabilities Accelerator (ASCA):** ASCA serves as the primary vehicle for funding and accelerating dual-use and asymmetric technology projects. It shifts the focus from traditional research grants to a “capability accelerator” model, where the government expects companies to co-invest and maintain a high level of readiness to transition innovation into usable military capability at an accelerated pace. By operating within the Vice Chief of the Defense Force Group, it ensures that technical developments are directly aligned with urgent warfighter needs and rapid acquisition cycles.
- **Defense Industry Development Strategy (DIDS):** The DIDS acts as a unified master plan that moves away from fragmented policies to position resilient supply chains as a core pillar of national defense policy. It explicitly prioritizes the growth of the defense industrial base through exports and commits to the expansion of the GSC program. By defining SDIPs, the DIDS ensures that domestic industrial capability in critical areas—such as autonomous systems and guided weapons—is developed to guarantee Australian freedom of action during strategic disruptions.

Aggregators and Co-Production: The GWEO Enterprise

The **Guided Weapons and Explosive Ordnance (GWEO) Enterprise** illustrates how Australia is operationalizing this new partnership model in practice.³² Recognizing that reliance on overseas stockpiles represented a strategic vulnerability, the government opted for a co-production approach rather than exclusive off-the-shelf procurement.

Under the GWEO model, global defense primes act as **industrial aggregators**, managing the transfer of intellectual property, technical data, and production know-how to Australian facilities. This enables Australia to progress from sustainment and assembly toward active co-production and, over time, more advanced manufacturing.

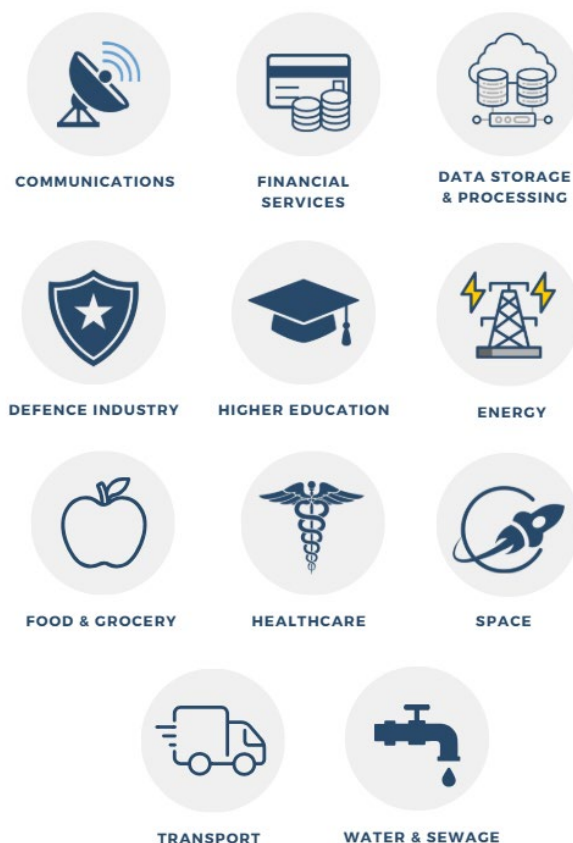
The GWEO Enterprise exemplifies how public-private cooperation can simultaneously strengthen sovereign capability, deepen allied integration, and maintain commercial viability for participating firms.

³² Department of Defence, n.d. “Guided Weapons and Explosive Ordnance Enterprise.” *Australian Government*. Accessed December 31, 2025. <https://www.defence.gov.au/business-industry/industry-capability-programs/guided-weapons-explosive-ordnance-enterprise>

Regulating for Resilience: The SOCI Framework

While ASCA and DIDS focus on building capability, the **SOCI framework** focuses on protecting it. Through successive legislative expansions since 2018, the SOCI regime now covers eleven critical sectors and imposes **positive security obligations** on asset owners and operators.³³

Figure 1. Critical Infrastructure Sectors



A key instrument within this framework is the **Critical Infrastructure Risk Management Program (CIRMP)**, which requires firms to assess and manage risks across cyber, physical, personnel, and supply chain domains. Importantly, CIRMP reporting must be approved at board level, elevating resilience from an operational concern to a matter of corporate governance and fiduciary responsibility.³⁴

Amendments introduced through the Enhanced Response and Prevention framework further empower the government to issue directions during severe incidents, including prioritizing deliveries or services. In effect, this deputizes private firms as instruments of national resilience under exceptional circumstances, while maintaining normal commercial autonomy in peacetime.

³³ Department of Defence. n.d. "Guided Weapons and Explosive Ordnance Enterprise." *Australian Government*. Accessed December 31, 2025. <https://www.defence.gov.au/business-industry/industry-capability-programs/guided-weapons-explosive-ordnance-enterprise>

³⁴ Ashurst (2024). SOCI CIRMP – are you ready? Legal Insight Series. <https://www.ashurst.com/en/insights/soci-cirmp-are-you-ready/>. Accessed 30 December 2025.

Table 2: The Private-Sector Obligations and Impact Under SOCI Legislation

Obligation	Description	Private-Sector Impact
Registration	Register assets on the Register of Critical Infrastructure Assets.	Administrative burden; creates government visibility of ownership structures.
Incident Reporting	Mandatory reporting of cyber incidents (12-72 hours).	Operational pressure to detect and report rapidly; connects private SOC's to ACSC.
CIRMP	Develop and maintain a Risk Management Program (Cyber, Physical, Personnel, Supply Chain).	Significant compliance cost; requires alignment with standards like ISO 27001.
Annual Reporting Cyber and Infrastructure Security Centre. 2024. "Cyber Security Legislative Reforms." <i>Department of Home Affairs</i> . Accessed December 31, 2025. https://www.cisc.gov.au/legislation-regulation-and-compliance/cyber-security-legislative-reforms .	Submit annual report approved by the Board.	Board Liability: Elevates security to a Director-level fiduciary duty.
Government Assistance	"Step-in" powers for government to intervene in a crisis.	Loss of operational control during extreme national security events.

Information Sharing and Engagement Challenges

Public-private cooperation is also supported through institutionalized information-sharing mechanisms, most notably the **Trusted Information Sharing Network (TISN)**. Organized around sector-specific groups, TISN facilitates the exchange of threat intelligence, best practices, and risk assessments between government agencies and critical infrastructure operators.³⁵

While widely regarded as essential, TISN and similar mechanisms face challenges related to engagement fatigue, uneven participation, and information asymmetries, particularly among smaller firms with limited compliance capacity. Australian authorities have acknowledged these constraints and are seeking to reinvigorate engagement through targeted outreach, sector-specific forums, and clearer articulation of the mutual benefits of participation.³⁶

³⁵ CISC (2024). Trusted Information Sharing Network (TISN). Cyber and Infrastructure Security Centre, Department of Home Affairs. <https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network>. Accessed 30 December 2025.

³⁶ ANAO (2022). Administration of Critical Infrastructure Protection Policy. Australian National Audit Office, Auditor-General Report No. 38 2021–22. <https://www.anao.gov.au/work/performance-audit/administration-critical-infrastructure-protection-policy>. Accessed 30 December 2025.

Assessment

Australia's public-private cooperation model reflects a pragmatic response to a more contested strategic environment. Rather than attempting to nationalize risk management or impose rigid state control, the government has focused on **shaping incentives, reducing barriers to collaboration, and embedding industry within trusted allied ecosystems**. This approach preserves market dynamics while recognizing that resilience and security are increasingly collective goods.

At the same time, the model places significant demands on private actors, particularly SMEs, in terms of compliance, cybersecurity, and governance. Managing these burdens while sustaining engagement will remain a central challenge as Australia continues to deepen its defense-industrial integration with trusted partners.

Governance Logic and Burden-Sharing Implications

Australia's public-private cooperation model in national defense and security is best understood as a **distributed governance system**, rather than a centrally commanded industrial policy. Responsibility for resilience is deliberately spread across government, prime contractors, and lower-tier suppliers, with the state acting primarily as an orchestrator of incentives, standards, and risk visibility.

At the strategic level, frameworks such as the **DIDS** and **SDIPs** define where domestic capability is essential and where reliance on trusted partners is acceptable. At the operational level, mechanisms such as **ASCA**, the **GSC Program**, and **GWEO** translate these priorities into concrete industrial participation and technology development pathways. At the regulatory level, the **SOCI** framework ensures that private-sector assets critical to national security are subject to minimum resilience and reporting standards.

This model deliberately avoids direct state ownership or comprehensive command-and-control mechanisms. Instead, it relies on **conditional participation**: firms retain commercial autonomy in normal circumstances but accept heightened obligations in exchange for access to defense markets, export opportunities, and long-term integration into allied supply chains.

Private-Sector Costs and Capability Constraints

While this model preserves market dynamics, it places significant demands on participating firms, particularly small and medium-sized enterprises. Compliance with export controls, cybersecurity requirements, supply chain risk management, and board-level accountability under SOCI legislation generates non-trivial costs. For SMEs, these obligations can represent a substantial barrier to entry, even when commercial opportunities are attractive.

The government has sought to mitigate these pressures through mentoring arrangements under the GSC Program, targeted capability uplift initiatives, and streamlined regulatory alignment with key allies. Nevertheless, the cumulative compliance burden remains a persistent challenge and contributes to uneven participation across regions and tiers of industry.

This tension reflects a broader structural issue inherent in trusted supply chain strategies: resilience and security are collective goods, but compliance costs are borne disproportionately by individual firms. Managing this imbalance without eroding incentives for participation remains one of the central governance challenges in Australia's public-private security model.

Implications for Trusted Supply Chains

Despite these constraints, Australia's public-private cooperation framework provides a credible model for embedding firms into **trusted defense and technology supply chains** without abandoning openness or competition. By combining strategic guidance, targeted incentives, and proportionate regulation, the government has created conditions under which private actors can align commercial strategies with national and allied security objectives.

The Australian case highlights that trusted supply chains are not built solely through trade restrictions or reshoring mandates. They emerge through **institutionalized cooperation**, predictable rules, and shared risk management between governments and firms. Australia's experience demonstrates both the potential and the limits of this approach, offering valuable lessons for other U.S. partners seeking to strengthen resilience while preserving private-sector dynamism.

Coordination Frictions and Implementation Risks

At the same time, Australia's model also highlights where trusted supply chain strategies can stall at the implementation layer. First, the governance system is dense and multi-instrument: firms must navigate overlapping requirements across procurement, export controls, critical infrastructure regulation, cybersecurity standards, and, increasingly, allied interoperability demands. For large primes this complexity is manageable; for SMEs, it can become a binding constraint that limits participation or pushes firms toward lower-risk, lower-value activities. Second, the "engagement fatigue" observed in information-sharing mechanisms such as TISN is not merely a communications problem, but it reflects a structural tension between the public interest in visibility and the private-sector concern about compliance exposure, reputational risk, and uneven burden-sharing. Third, visibility into Tier-2 and Tier-3 dependencies remains uneven, meaning that resilience gains at the top of the supply chain do not automatically translate into system-wide robustness.

Key takeaway: Trusted Supply Chains Require a Workable Bargain

For the purposes of this project, Australia illustrates a broader lesson: trusted supply chains are not built simply through political alignment or declarations of partnership, but through **institutionalized cooperation that creates a workable bargain for firms**. That bargain typically has three parts: (i) clarity and predictability in rules and expectations; (ii) proportionality in compliance burdens, especially for SMEs; and (iii) tangible value for participation, such as access to export pipelines, capability uplift support, or integration into long-term allied work packages. Where these conditions are met, firms are more likely to internalize security objectives as part of commercial strategy rather than treating them as externally imposed constraints.

Overall, Australia's experience demonstrates how a U.S. partner can pursue economic security through integration into trusted allied ecosystems while remaining outward-

oriented and market-based. The central policy challenge going forward is not whether public-private cooperation is necessary—it is—but how to keep cooperation sustainable by aligning incentives, reducing unnecessary friction, and ensuring that trusted supply chain requirements remain compatible with competitiveness and innovation.

2.2.6 Conclusion

Australia's evolving approach to economic security and trusted supply chains reflects a pragmatic recalibration of a traditionally open, trade-dependent economic model to the realities of a more contested geoeconomic environment. Rather than pursuing broad decoupling or protectionist restructuring, Australia is seeking to manage strategic vulnerabilities through a layered policy architecture that combines selective industrial policy, risk-based regulation, and alliance-based integration, while maintaining a continued commitment to global markets and a rules-based international economic order.

At the economic policy level, Australia's frameworks increasingly embed security considerations into decisions on investment, supply chains, and industrial capability. The Future Made in Australia agenda, together with the National Interest Framework, demonstrates an emerging preference for disciplined, criteria-based intervention aimed at addressing concentrated dependencies and strengthening domestic capability where it materially contributes to resilience. Importantly, these measures are framed not as a rejection of openness, but as an effort to ensure that openness does not translate into unmanageable exposure in critical sectors. Complementary initiatives, including critical minerals strategies, reforms to foreign investment screening, and regional diversification efforts, illustrate a whole-of-economy approach to de-risking that seeks to broaden partnerships and reduce excessive concentration without abandoning Australia's outward orientation.

In the defense and dual-use domain, Australia's policy trajectory is even more clearly anchored in trusted supply chain integration with allied ecosystems. The 2023 Defense Strategic Review and 2024 National Defense Strategy elevate supply chain resilience from an operational concern to a strategic requirement. These priorities are operationalized through instruments such as the Defense Industry Development Strategy, capability acceleration via ASCA, co-production initiatives such as the GWEO Enterprise, and regulatory strengthening through the Security of Critical Infrastructure framework. Together, these measures reflect a shift from a narrow procurement logic toward a more integrated model of defense-industrial preparedness, in which firms are treated as contributors to sovereign capability and national resilience.

Australia's alliance-based approach is further institutionalized through mechanisms that formalize trusted interdependence. The Security of Supply Arrangement with the United States, alongside complementary trade facilitation frameworks and the deeper industrial and technology integration pursued through AUKUS, collectively reinforces the expectation that resilience can be achieved through structured cooperation rather than self-sufficiency. In practice, this approach seeks to secure assured access to critical inputs and capabilities during crises, strengthen interoperability, and enable Australian firms to participate more deeply in allied production and innovation networks.

A distinctive strength of the Australian model is its emphasis on **resilience-through-integration**. The Global Supply Chain Program illustrates this logic in concrete terms:

embedding Australian SMEs into the supply chains of allied primes creates durable, repeat relationships that strengthen both commercial viability and strategic readiness. Rather than relying on one-off local content measures, the program aims to position Australian firms as trusted nodes in longer-term allied production ecosystems. This has clear relevance for trusted supply chain cooperation among the United States and its partners, particularly where resilience requires not only secure sourcing but also sustained capability across tiers of suppliers.

At the same time, Australia's experience highlights several recurring implementation challenges that are directly relevant to public-private coordination. Compliance burdens and regulatory complexity can be manageable for large primes but disproportionately constraining for SMEs, potentially limiting participation or reducing incentives to move into higher-value segments. Mechanisms for information sharing and collective preparedness such as TISN remain important but are vulnerable to engagement fatigue and persistent tensions around disclosure, liability, and uneven burden-sharing. In addition, while Australia's policy architecture improves visibility and resilience at higher tiers of defence supply chains, systemic vulnerability often concentrates further downstream, where Tier-2 and Tier-3 dependencies remain harder to map and mitigate.

Overall, Australia's case suggests that trusted supply chain cooperation is most durable when it is underpinned by a workable institutional bargain for firms: predictable rules, proportionate compliance expectations, and tangible participation value (such as export pipeline access, capability uplift, or long-term integration into allied programs). Australia's policy direction is clear and increasingly coherent, but sustained success will depend on managing the trade-offs between resilience and competitiveness, reducing friction for SMEs, and translating high-level coordination objectives into operationally usable frameworks across the supply chain.

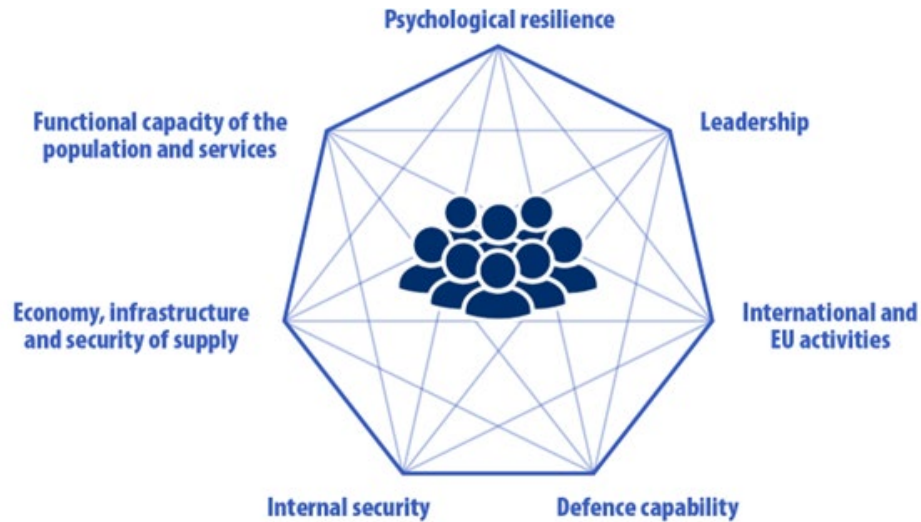
2.3 Finnish Government Policies for Economic Security and Trusted Supply Chains

Finland's approach to economic security and trusted supply chains is shaped by a distinctive combination of structural openness and strategic vulnerability. As a small, highly trade-dependent economy located at the geopolitical frontier of Europe, Finland has long been acutely aware of its exposure to external disruptions in critical flows of energy, materials, goods, and information. This awareness has produced a policy model that combines a strong commitment to open, rules-based international markets with an unusually developed system of preparedness, resilience, and security of supply.

At the core of this model lies Finland's Comprehensive Security concept, which frames economic security as an integral component of national resilience rather than a standalone industrial or trade policy objective. Formalized through successive iterations of the Security Strategy for Society (2012, 2017, 2025), Comprehensive Security identifies seven vital societal functions: leadership; international and European Union (EU) activities; defense capability; internal security; economy, infrastructure and security of supply; functional capacity of the population and services; and psychological resilience.

These functions are secured through close cooperation between government authorities, the private sector, and civil society.³⁷

Figure 2. Vital Functions of the Society



Security of Supply occupies a central place within this framework. Unlike narrower interpretations found in many countries, Finland's concept of security of supply encompasses not only critical materials and industrial inputs, but also infrastructure, services, logistics, energy, food systems, pharmaceuticals, and other functions essential to societal continuity and national defense. Importantly, this is not a state-centric model. Instead, it is explicitly collaborative, relying on structured public-private cooperation to ensure preparedness, continuity, and rapid response during crises.

Finland's security doctrine has evolved over decades in response to both geopolitical realities and historical experience. During the Cold War and subsequent decades of military non-alignment, policy focused on ensuring extended national autonomy under conditions of disruption, including the ability to sustain society and defense for prolonged periods in the event of embargoes or conflict. This approach was institutionalized in the 1960s through the Total Defense model and later broadened in the 1990s to reflect post-Cold War globalization and the growing complexity of civilian dependencies. The establishment of the NESO and its public-private counterpart, NESO, marked a shift toward managing interdependence rather than attempting to eliminate it.³⁸

EU membership in 1995, accelerating globalization, and the digitalization of the Finnish economy further transformed the model. The emphasis moved away from purely material stockpiling toward continuity management, supply chain resilience, and systemic risk governance across increasingly interconnected value chains. The Russian invasion of Ukraine in 2022 then marked a decisive inflection point, triggering a rapid reassessment of Finland's security posture and accelerating the integration of

³⁷ The Security Committee, "Vital Functions of the Society", <https://turvallisuuskomitea.fi/en/security-strategy-for-society/vital-functions/>

³⁸ NESO, "Historic view", <https://www.huoltovarmuuskeskus.fi/en/organisation/historic-view/1990s>

economic security into allied defense and resilience frameworks. Finland's NATO accession in April 2023 and the subsequent entry into force of the DCA with the United States in September 2024 have reinforced a transition from a model centered on national autonomy toward one based on trusted interdependence with allies, shaping not only defense policy, but also the governance of critical supply chains and economic resilience.

2.3.1 Strategic Foundations: Comprehensive Security and Trusted Interdependence

While Finland's approach to economic security is often described through its specific institutions, its deeper logic lies in a strategic conception of security that integrates economic, societal, and defense considerations into a single framework. The Comprehensive Security model provides this foundation, treating economic resilience and supply chain continuity as preconditions for national security rather than secondary policy objectives.

Comprehensive Security is codified through Finland's Security Strategy for Society, most recently updated in January 2025.³⁹ The strategy reflects a shift from crisis preparedness as a contingency activity toward resilience as a permanent feature of governance. Rather than assuming that disruptions are exceptional events, Finnish policy assumes that shocks, whether geopolitical, economic, technological, or hybrid, are a recurring feature of the operating environment. As a result, preparedness, continuity, and risk management are embedded across policy domains and administrative levels.

A defining feature of this approach is its rejection of strict self-sufficiency as a viable or desirable objective. Historically, Finland's security doctrine placed heavy emphasis on national autonomy, reflecting Cold War realities and prolonged periods of military non-alignment. Over time, however, policymakers concluded that autonomy alone could not provide adequate protection in an era of deep economic interdependence and complex value chains. Instead, Finland has progressively reoriented toward a model of managed and trusted interdependence, in which resilience is achieved through a combination of domestic capability, diversification, and institutionalized cooperation with reliable partners.⁴⁰

This strategic reorientation has accelerated markedly since 2022. Finland's accession to NATO in April 2023 represents not only a military alignment, but a broader shift in how security of supply is conceptualized. Membership in the alliance embeds Finland within a collective defense and logistics system, reducing the need to duplicate capabilities that can be accessed through trusted partners. At the same time, it increases the importance of interoperability, standardization, and reliability across defense-related supply chains.

The DCA with the United States exemplifies this logic. By enabling the pre-positioning of U.S. materiel on Finnish territory and deepening operational integration, the DCA signals a move away from autonomy as insulation toward autonomy through access. In

³⁹ Finland's comprehensive security reinforced through new security strategy for society. https://www.defmin.fi/en/topical/press_releases_and_news/finland_s_comprehensive_security_reinforced_throug_h_new_security_strategy_for_society.14801.news

⁴⁰ Finland's de-risking and supply security, <https://www.huoltovarmuuskus.fi/files/c1a60bd184e062b22b23bc3739abd295feb8f11d/hvk-de-risking-tilannekuva-eu-ja-suomi-saavutettava.pdf>

economic security terms, this translates into a preference for anchoring critical supply chains within allied frameworks where access, priority, and mutual assurance can be institutionalized rather than improvised during crises.

Crucially, Finland's approach does not frame trusted interdependence as a zero-sum choice between openness and security. Instead, it seeks to preserve Finland's position as an open, export-oriented economy while selectively governing those dependencies that could translate into strategic vulnerability. Comprehensive Security thus functions as a filtering mechanism: openness is maintained where risks are manageable, while critical functions are subject to higher standards of preparedness, redundancy, and coordination.

This strategic foundation shapes all subsequent policy choices from institutional design and external alignment to corporate obligations and incentives. Trusted supply chains in the Finnish context are therefore not primarily the result of trade policy or industrial subsidies, but of a long-standing security doctrine that treats economic resilience as a collective responsibility shared between the state and the private sector.

2.3.2 External Alignment: EU, NATO, the United States, China, and Regional Partners

Finland's economic security strategy is shaped not only by domestic institutions, but by a deliberate effort to anchor resilience within a broader network of external partnerships. As a small, open economy, Finland recognizes that trusted supply chains cannot be sustained through national measures alone. Instead, diversification, alliance integration, and institutional alignment function as core instruments for managing risk in an increasingly fragmented global environment.

European Union: Shaping Collective Resilience Without Centralization

Within the EU, Finland supports efforts to strengthen strategic competitiveness and economic security, particularly through the identification and management of critical dependencies in areas such as energy, advanced technologies, and critical raw materials. At the same time, Finland consistently emphasizes that these objectives should be pursued through market-based mechanisms and respect for subsidiarity and proportionality.

Finnish policymakers remain cautious about excessive centralization of economic security governance at the EU level. This reflects both constitutional principles and practical experience: Finland views its nationally embedded Comprehensive Security and security-of-supply model as more effective than ad hoc or highly centralized crisis instruments. As a result, Finland seeks to influence EU policy by promoting its approach as a reference model rather than by advocating wholesale transfer of authority to the European Commission.

This logic is evident in Finland's support for the emerging concept of a European Preparedness Union, articulated in a 2024 report led by former President Sauli Niinistö⁴¹. The initiative draws heavily on Finnish experience, emphasizing anticipation, continuity planning, and public-private cooperation rather than protectionism or

⁴¹ Safer together: A path towards a fully prepared Union, https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en

permanent emergency measures. Finland's strategy thus combines active participation in EU economic security initiatives with a firm insistence on preserving effective national governance structures.

NATO and the United States: Anchoring Security of Supply Through Allied Integration

Finland's accession to NATO in April 2023 has fundamentally reshaped its external economic security environment. Beyond collective defense guarantees, NATO membership embeds Finland within allied logistics, procurement, and industrial ecosystems, increasing the importance of interoperability and assured access to critical inputs.

The DCA with the United States, which entered into force in September 2024, represents a central pillar of this integration. The agreement enables the pre-positioning of U.S. materiel on Finnish territory and deepens cooperation across logistics, infrastructure, and sustainment. From an economic security perspective, the DCA institutionalizes access to allied capacity and reduces the need for Finland to replicate expensive capabilities domestically.

This cooperation is reinforced by the long-standing SOSA between Finland and the United States, in place since 2007.⁴² The SOSA provides a framework for mutual priority access to defense-related goods and services, enhancing predictability and assurance during crises. Together, NATO membership, the DCA, and the SOSA create a stable institutional environment in which firms can rationally prioritize reliability and trusted sourcing over short-term cost efficiency.

For Finnish companies operating in sensitive or defense-adjacent sectors, these arrangements increasingly shape commercial strategy. Alignment with transatlantic security frameworks functions as both a risk-management mechanism and a credibility signal within allied supply chains.

China: De-Risking Through Selective Engagement

Finland's relationship with China illustrates the balancing logic at the heart of its economic security approach. China remains an important trading partner, and Finnish policy does not seek broad disengagement. At the same time, authorities increasingly recognize that certain economic, technological, and industrial dependencies may expose society to coercive leverage or strategic vulnerability.

This assessment is articulated in Finland's Action Plan on China (2025-2029)⁴³ and reinforced in foreign and security policy reviews. The emphasis is on de-risking rather than decoupling: reducing exposure in critical sectors, strengthening screening of sensitive investments, and ensuring that dependencies are transparent and governable.

In practice, this means maintaining commercial engagement in lower-risk domains while exercising caution in areas involving critical infrastructure, advanced technologies, or dual-use capabilities. Finland's approach reflects a broader European

⁴² Department of Defense, "Security of Supply", <https://www.businessdefense.gov/security-of-supply.html>

⁴³ Joint Action Plan between China and Finland 2025-2029, https://finlandabroad.fi/web/chn/current-affairs/-/asset_publisher/h5w4iTUJhNne/content/joint-action-plan-between-china-and-finland-2025-2029/35732

trend, but is shaped by its proximity to Russia, its alliance commitments, and its comprehensive understanding of societal vulnerability.

Nordic and Like-Minded Partnerships

Regionally, Nordic cooperation has intensified significantly since 2022. The Nordic Defense Cooperation provides a flexible framework for joint planning, exercises, and capability development, allowing both multilateral and targeted bilateral initiatives. This flexibility aligns well with Finland's preference for practical, modular cooperation over rigid institutional structures.

Beyond the Nordic region, Finland has deepened cooperation with other technologically advanced, trade-dependent democracies facing similar challenges, including Canada, Australia, South Korea, and Japan. These partnerships support diversification of supply chains and exchange of best practices on resilience, dual-use governance, and public-private coordination.

The 2024 Icebreaker Collaboration Effort (ICE Pact) between Finland, the United States, and Canada exemplifies this approach in a strategically sensitive domain. By leveraging Finland's specialized expertise in ice-capable shipbuilding, the agreement strengthens trusted industrial cooperation in the Arctic while addressing emerging geopolitical and logistical risks linked to climate change and increased maritime activity.

External Alignment as a Pillar of Trusted Supply Chains

Taken together, Finland's external alignment strategy reflects a coherent approach to trusted supply chains: resilience is built not through insulation, but through institutionalized cooperation with reliable partners. By embedding its economic security within EU, NATO, and transatlantic frameworks, while maintaining diversified global engagement, Finland seeks to reduce vulnerability without sacrificing openness. This external orientation complements Finland's domestic institutional architecture, anchoring security of supply in predictable, rule-based, and trusted international relationships.

2.3.3 Institutional Architecture for Security of Supply and Trusted Supply Chains

Finland's approach to economic security and trusted supply chains is distinguished not by isolated policy instruments, but by the institutionalization of resilience as a permanent feature of economic governance. Rather than relying on ad hoc task forces, crisis-driven interventions, or short-term industrial programs, Finland has developed a standing institutional architecture that integrates public authorities and private firms into a continuous system of anticipation, coordination, and preparedness.

At the center of this architecture is the **NESA**, which functions as a dedicated authority responsible for coordinating security of supply across the Finnish economy. Unlike many counterparts in other advanced economies, NESA is neither a purely advisory body nor a narrow stockpiling agency. It combines strategic foresight, coordination authority, asset ownership, and public-private governance into a single institutional node, making it a cornerstone of Finland's trusted supply chain model.

Table 3. Roles and Responsibilities

Actor	Role	Key Functions
Finnish Government	Policy and Strategic Direction	Adopts and updates the Security Strategy for Society; manages key international relationships (e.g., NATO, EU, U.S.); sets overall fiscal policy and defense spending
Ministry of Economic Affairs and Employment	Ministerial Oversight	Parent ministry for NESAs; provides a policy direction for Security of Supply, foreign direct investment (FDI) screening and economic policies
National Emergency Supply Agency (NESA)	Central Coordinating Body	Maintains strategic reserves; holds stakes in critical companies; fosters public-private collaboration through NESO; conducts foresight and risk analysis
Private Sector Companies	Operational Resilience	Implement supply chain resilience practices (e.g., multi-sourcing, inventory); engage in NESA's network and contribute to strategic planning; may voluntarily absorb higher costs for friendshoring

NESA as a Permanent Economic Security Authority

NESA operates under the Ministry of Economic Affairs and Employment and is tasked with safeguarding the continuity of critical economic and societal functions under conditions of disruption, crisis, or conflict. Its remit extends across energy, food, healthcare, transport, digital infrastructure, finance, and key industrial sectors deemed essential to national resilience and defense.

A defining feature of NESA's mandate is its ex-ante orientation. Rather than focusing primarily on emergency response, NESA systematically maps dependencies, identifies vulnerabilities, and coordinates preparedness measures before shocks materialize. This forward-looking posture differentiates Finland's model from approaches that rely heavily on post-crisis intervention or temporary emergency powers.

NESA exercises its mandate through a combination of complementary tools, including:

- **Strategic stockpiling**, covering fuels, grains, pharmaceuticals, fertilizers, and selected industrial inputs;
- **Coordination of preparedness obligations**, combining mandatory requirements with voluntary commitments agreed in cooperation with industry;
- **Foresight and risk analysis**, including scenario planning, stress testing, and dependency mapping across critical value chains;
- **Selective ownership stakes** in strategically critical infrastructure, most notably a significant minority share in the national electricity transmission operator, Fingrid.⁴⁴

⁴⁴ State corporate holdings 2024, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166334/VN_2025_62.pdf?sequence=1&isAllowed=y

This mix allows Finland to secure continuity of supply not by displacing markets, but by structuring market behavior around resilience objectives and long-term continuity.

The National Emergency Supply Organization (NESO): Standing Public-private Governance

Operational cooperation between the state and industry is organized through **NESO**, a structured public-private network coordinated by NESO. NESO operationalizes the principle that trusted supply chains cannot be imposed solely through regulation or incentives, but must be co-produced with firms that control critical assets, capabilities, and knowledge.

NESO is organized into seven sectors and twenty-seven industry-based pools, covering areas such as energy, logistics, healthcare, food supply, information and communication technology (ICT), manufacturing, and finance. These pools bring together public authorities and selected private firms deemed critical to societal functioning. Participation is voluntary, but once engaged, firms commit to meaningful preparedness obligations.

Unlike conventional consultation mechanisms, NESO pools function as standing governance bodies rather than episodic advisory groups. They:

- conduct joint risk assessments and contingency planning;
- participate in regular exercises and simulations;
- develop sector-specific preparedness standards and best practices;
- enable trusted information sharing under protected conditions.

For firms, participation provides early access to risk information, coordination with peer companies, and direct linkage to government planning. For the state, it ensures that resilience policy is grounded in operational reality and that vulnerabilities are identified well below Tier-1 suppliers, where disruptions often originate.

Corporate Integration and Governance Incentives

Finland's institutional architecture deliberately embeds economic security considerations within corporate decision-making rather than treating firms as external implementers of government policy. This integration is reinforced through several governance mechanisms.

First, continuity management is treated as a core business responsibility for firms participating in NESO pools. Companies are expected to maintain preparedness plans, assess supply chain dependencies, and ensure continuity of essential services under stress. While not all requirements are legally mandated, expectations are reinforced through peer benchmarking, sectoral norms, and reputational incentives.

Second, private-sector interests are formally represented in governance. By statute, at least four of the eleven members of NESO's board must represent private-sector organizations.⁴⁵ This ensures that corporate perspectives shape national preparedness

⁴⁵ Members were chosen based on nominations by the NESO Council and formally confirmed by the Finnish Government. Following a legislative change, effective 1 April 2026, the Board will be replaced by an inter-ministerial

priorities while simultaneously binding firms into collective responsibility for resilience outcomes.

Third, NESAs's selective equity stakes in critical infrastructure firms constitute a distinctive governance tool. Rather than relying solely on regulation or public ownership, Finland uses minority ownership to align incentives, secure long-term investment horizons, and retain strategic oversight in sectors where continuity is non-negotiable.

Trusted Supply Chains Through Structured Interdependence

Finland's institutional architecture reflects a strategic choice to pursue trusted interdependence rather than self-sufficiency. This logic has been reinforced since Finland's NATO accession and deepening integration with transatlantic security frameworks. The Defense Cooperation Agreement with the United States and Finland's long-standing SOSA exemplify this shift toward institutionalized access and mutual assurance.

Within this framework, trusted supply chains are defined less by geography or ownership nationality than by institutional reliability. Firms operating within Finland's security-of-supply ecosystem are expected to meet high standards of transparency, preparedness, and cooperation. Dependencies that cannot be governed through such trusted arrangements are systematically reduced, diversified, or hedged.

This approach allows Finland to remain a highly open, export-oriented economy while maintaining a high level of resilience in critical sectors. Rather than fragmenting supply chains wholesale, Finland selectively governs key nodes and flows, ensuring that openness does not translate into strategic vulnerability.

2.3.4 Corporate Trade-Offs, Incentives, and Burdens in Finland's Trusted Supply Chain Model

While Finland's security-of-supply system is often presented as a best-practice model of public-private cooperation, it imposes real and non-trivial trade-offs on participating firms. Trusted supply chains in the Finnish context are not cost-neutral, nor are they sustained purely by normative alignment or patriotic commitment. Instead, they rest on a negotiated balance between commercial autonomy, resilience obligations, and strategic access.

Understanding these trade-offs is essential for assessing both the durability of the Finnish model and the conditions under which its core principles might be transferable to other contexts.

Cost Absorption and the "Resilience Premium"

For firms embedded in Finland's security-of-supply ecosystem, resilience entails measurable and ongoing costs. Participation in NESO pools typically requires companies to:

steering group. Whilst not confirmed yet, the stated intent is to nominate 2 private sector representatives in this new body.

- maintain higher inventory levels than those implied by market-optimal just-in-time models;
- diversify sourcing even where single-supplier arrangements would be cheaper;
- invest in continuity management, redundancy, cybersecurity, and crisis preparedness that may not be utilized in normal operations;
- allocate senior management time to planning, exercises, and coordination activities that do not directly generate revenue.

Together, these measures create what many firms implicitly treat as a **“resilience premium”** – a structural cost absorbed in exchange for systemic stability and long-term operating certainty. Importantly, this premium is not consistently offset through direct subsidies or compensation. Unlike more interventionist industrial-policy models, Finland relies less on financial incentives and more on indirect, relational forms of return.

Why Firms Participate Despite the Costs

Despite these burdens, corporate participation in Finland's trusted supply chain framework has remained relatively stable over time. This persistence reflects a combination of strategic, informational, and reputational incentives.

First, firms gain **predictability and early warning**. Through NESO pools and NESA coordination, participating companies receive access to forward-looking risk assessments, scenario planning, and privileged situational awareness. In an environment of heightened geopolitical volatility, this informational advantage has become strategically valuable.

Second, participation confers **status as a trusted operator** within national and allied security frameworks. Firms embedded in the security-of-supply system are implicitly recognized as reliable partners during crises, which can translate into preferential access to coordination mechanisms, emergency logistics support, and in certain circumstances priority engagement with public authorities.

Third, for export-oriented firms in critical or dual-use sectors, alignment with Finland's preparedness regime increasingly functions as a **credibility signal** vis-à-vis international partners. Compliance with Finnish continuity and resilience standards can strengthen firms' positioning within EU, NATO, and transatlantic supply chain cooperation, particularly in defense-adjacent and high-reliability markets.

Asymmetric Burdens and SME Constraints

The costs associated with trusted supply chains are not evenly distributed. Large incumbent firms are generally better positioned to absorb resilience investments and governance obligations. SMEs, however, face proportionally higher challenges.

For SMEs, participation can strain limited managerial and financial capacity:

- continuity planning and reporting requirements may exceed available resources;
- investments in redundancy, cybersecurity, and compliance can crowd out growth-oriented spending;

- participation in preparedness exercises imposes opportunity costs that are harder to justify commercially.

This creates a structural tension within the Finnish model. SMEs are often critical Tier-2 and Tier-3 suppliers, yet they are also the least equipped to bear additional resilience obligations. To mitigate this, NESO and industry associations emphasize graduated expectations, peer learning within pools, and targeted support measures. Nevertheless, the asymmetry remains a constraint, particularly in sectors where supply chain fragility is concentrated below prime contractors.

Voluntariness, Trust, and Path Dependence

A defining feature of Finland's approach is the voluntary nature of corporate participation. Firms are not legally compelled to join NESO pools, yet withdrawal is rare. This stability rests on high levels of institutional trust and a long-standing tradition of cooperation between the state and industry.

At the same time, this reliance on trust creates **path dependence**. The model functions effectively because it has evolved over decades and is embedded in Finland's political culture and governance norms. Replicating it elsewhere would require more than regulatory reform; it would demand sustained credibility, predictable reciprocity, and visible commitment from the state.

From a corporate perspective, participation is sustained less by short-term commercial returns than by a shared understanding that resilience is a collective good that protects long-term operating conditions. This logic may be harder to sustain in environments characterized by lower trust or more adversarial state-business relations.

Strategic Trade-Off: Autonomy Versus Embeddedness

At a deeper level, Finland's trusted supply chain model involves a strategic trade-off between corporate autonomy and institutional embeddedness. Firms retain ownership, market access, and commercial freedom, but in exchange accept deeper integration into national preparedness structures and, increasingly, allied security frameworks.

Following Finland's NATO accession and deepening transatlantic integration, this trade-off has become more pronounced. For firms operating in sensitive sectors, alignment with Finland's security-of-supply expectations increasingly entails alignment with broader Western economic security priorities. While this enhances stability and access to trusted markets, it may constrain strategic optionality in politically sensitive or high-growth regions.

Taken together, these trade-offs highlight both the strength and the limits of Finland's model. Trusted supply chains are sustained not by mandates alone, but by carefully balanced incentives, credible governance, and long-term alignment between state objectives and corporate strategy.

2.3.5 Limits, Vulnerabilities, and Transferability of the Finnish Model

Finland's security-of-supply and trusted supply chain framework is widely regarded as a best-practice example of institutionalized public-private cooperation in economic security. While this reputation is well founded, the model is not without limitations, nor

is it universally transferable. Understanding these constraints is essential both for realistic policy learning and for avoiding overextension of the concept beyond the conditions that make it effective.

Dependence on High Institutional Trust

A foundational precondition of the Finnish model is exceptionally high levels of institutional trust between the state, the private sector, and society at large. Firms participate voluntarily in preparedness structures not because of legal compulsion, but because they trust that:

- obligations will remain proportionate and predictable;
- sensitive commercial and security-related information will be handled responsibly;
- the state will reciprocate during crises rather than impose unilateral burdens.

This trust has been built over decades through consistent governance practices, transparency, and a political culture that frames resilience as a shared societal responsibility. In environments where trust in public institutions is weaker, or where state–business relations are more adversarial, similar voluntary mechanisms may fail to generate sustained engagement or credible preparedness.

Scalability and the Small-State Advantage

Finland's size constitutes both a strength and a constraint. As a relatively small economy with a concentrated industrial base, Finland can:

- maintain detailed visibility over critical firms and sectors;
- coordinate planning across a manageable number of actors;
- conduct meaningful joint exercises without excessive transaction costs.

Larger or more fragmented economies may struggle to replicate this level of coordination without creating heavy bureaucratic overhead, diluting accountability, or discouraging participation. The Finnish model benefits from administrative density and proximity between key actors—features that do not scale easily. This raises important questions about whether trusted supply chains in larger economies should rely on centralized coordination or instead adopt modular, sector-specific architectures.

Risk of Over-Securitization

Another vulnerability lies in the potential for over-securitization of economic activity. While Finland has so far maintained a careful balance between openness and preparedness, expanding security-of-supply logic into too many sectors risks:

- distorting market incentives;
- discouraging foreign investment;
- normalizing exceptional measures outside genuine crisis scenarios.

Finnish policymakers are acutely aware of this risk and have repeatedly stressed that security-of-supply measures must remain targeted, proportionate, and market-

compatible. Nevertheless, sustained geopolitical tension and heightened threat perceptions may increase pressure to broaden the scope of preparedness, testing the model's internal discipline over time.

Exposure Through Allied Integration

Paradoxically, Finland's deep integration with trusted allies also introduces new forms of dependence. NATO membership, the Defense Cooperation Agreement with the United States, and participation in transatlantic supply chains enhance security but also:

- increase reliance on allied production capacity and logistics;
- expose firms to extraterritorial regulatory regimes;
- align Finnish economic security more closely with broader Western strategic priorities.

While this integration is a deliberate strategic choice, it reduces Finland's ability to remain fully neutral in economic disputes involving major powers. For firms, this may constrain market access and strategic flexibility in certain regions, particularly where geopolitical tensions intersect with commercial opportunity.

Transferability: Principles Rather Than Templates

Taken together, these limitations suggest that the Finnish model should not be treated as a template to be copied wholesale, but as a set of design principles adaptable to local conditions. The most transferable elements are not specific institutions, but underlying governance logics:

- early integration of the private sector into risk assessment and preparedness;
- clear prioritization of genuinely critical functions;
- voluntary participation anchored in credible reciprocity;
- deliberate separation of preparedness from protectionism.

The Finnish case illustrates that trusted supply chains are ultimately a governance challenge rather than a technical one. Their durability depends less on the choice of policy instruments than on the quality of state-business relations, institutional credibility, and long-term policy consistency.

2.3.6 Policy on Dual-Use Technologies

Finland has adopted a proactive and increasingly assertive approach to governing dual-use technologies, reflecting their growing importance for both economic competitiveness and national security. As technological innovation becomes more tightly intertwined with defense capability and strategic advantage, Finnish policymakers have moved to ensure that open innovation ecosystems do not translate into unmanaged security risks.

In addition to implementing European Union-level export controls on dual-use items, Finland has introduced **national controls that go beyond the EU framework**. These measures extend authorization requirements to selected advanced technologies not

yet comprehensively regulated at the EU level, including advanced semiconductors, quantum computing technologies, and certain categories of manufacturing equipment. The objective is to close regulatory gaps that could otherwise allow sensitive capabilities to be transferred in ways that undermine national or allied security interests.

A distinctive feature of Finland's approach is the discretionary authority granted to the Ministry for Foreign Affairs to impose controls based on **end-use risk**, even where specific items are not listed. Exports may be restricted if their use could cause serious harm to Finland's public security or national defense. This risk-based mechanism allows for flexibility and anticipatory governance in fast-moving technological domains, where static control lists quickly become outdated.

At the same time, Finland has sought to avoid framing dual-use governance purely in restrictive terms. Export controls are complemented by policies designed to **strengthen domestic dual-use innovation capacity** and integrate Finnish firms into trusted technology ecosystems. National AI strategies emphasize ethical, secure, and responsible deployment across both civilian and defense applications, while targeted initiatives—such as the *Dual-use Discovery* program—support SMEs in identifying defense-relevant applications of civilian technologies and navigating regulatory and market barriers.

FDI screening reinforces this framework. While Finland's FDI regime remains comparatively liberal, ongoing reforms aim to better reflect heightened security concerns linked to advanced technologies and Finland's NATO membership. Oversight focuses on preventing the transfer of strategic influence, sensitive know-how, or critical capabilities to actors whose interests may conflict with Finland's security objectives.

Taken together, Finland's dual-use technology policy reflects a calibrated approach: openness to innovation and international collaboration is preserved, but bounded by governance mechanisms that prioritize trust, transparency, and alignment with allied security frameworks. In the context of trusted supply chains, this ensures that technological interdependence enhances resilience rather than creating new vectors of vulnerability.

2.3.7 Conclusion

Finland offers a distinctive and mature model of economic security grounded in preparedness, institutionalized public-private cooperation, and a clear understanding of interdependence as both a risk and a resource. Its evolution from a strategy centered on national autonomy toward one anchored in trusted interdependence with allies illustrates how supply chain resilience can be strengthened without abandoning openness or market principles.

The Finnish case demonstrates that trusted supply chains are not primarily the product of trade policy or industrial subsidies, but of **governance design**. By embedding resilience into permanent institutions, integrating private actors into risk assessment and preparedness, and anchoring national policy within credible allied frameworks, Finland has created a system in which security objectives are internalized by firms rather than imposed episodically by the state.

At the same time, the model's effectiveness rests on conditions that are not universally present: high institutional trust, administrative proximity, and a political culture that treats resilience as a collective responsibility. These features limit direct transferability but enhance the value of Finland as a source of design principles rather than policy templates.

For economies seeking to strengthen trusted supply chains in a more fragmented global environment, Finland's experience highlights a central lesson: resilience is sustained not by insulation from global markets, but by **governed openness**, a deliberate balance between economic integration, institutional trust, and strategic coordination with reliable partners.

2.4 South Korean Government Policies for Economic Security and Trusted Supply Chains

South Korea has placed supply chain governance at the center of its economic security strategy. Like other advanced manufacturing economies, it was affected by COVID-19 disruptions and by the broader destabilization of global value chains under intensifying U.S.-China strategic competition. What makes the South Korean case distinctive, however, is the degree to which **direct experiences of economic coercion and targeted supply restrictions** accelerated institutional change. China's de facto retaliatory measures following the 2016 Terminal High Altitude Area Defense (THAAD) deployment decision and Japan's 2019 export controls on key semiconductor-related materials strengthened a policy consensus in Seoul: supply chain resilience is no longer only an efficiency challenge, but a strategic vulnerability with national security implications.

In response, South Korea has pursued an economic security approach that combines **capability-building** with **risk governance**. On the capability side, it has sought to strengthen domestic competitiveness in strategically exposed upstream nodes, particularly "materials, parts, and equipment" (so-bu-jang), and to reinforce technological advantage in advanced industries such as semiconductors, batteries, and selected dual-use domains. On the governance side, it has moved to institutionalize supply chain risk management through dedicated legislation, standing coordination bodies, early-warning functions, and targeted financial instruments designed to support diversification and stabilization.

This supply chain posture is also shaped by South Korea's security environment. The persistent North Korean threat reinforces a more integrated understanding of security, in which economic resilience, cyber and infrastructure protection, and defense-industrial readiness increasingly intersect. As a result, economic security policymaking has shifted toward a more comprehensive and coordinated model, with supply chains treated as critical national infrastructure rather than as a purely commercial arena.

The following sections outline (1) the main features of South Korea's economic security strategy, (2) the core instruments and governance mechanisms underpinning supply chain stabilization, and (3) the public-private architecture supporting defense-industrial resilience and trusted supply chain cooperation.

2.4.1 Major Features of South Korea's Economic Security Strategy

South Korea's economic security strategy is best understood as an **evolution of its long-standing developmental and industrial policy tradition**, adapted to a more contested and risk-prone global environment. While recent policy innovations are substantial, they build on established patterns of state–industry coordination, export-oriented growth, and technology-driven competitiveness. At the same time, repeated exposure to external shocks and coercive measures has pushed South Korea to expand the scope of economic security beyond competitiveness alone, toward the mitigation of structural vulnerabilities within critical supply chains.

Industrial Policy as the Core Instrument

Industrial policy has historically been the central pillar of South Korea's economic strategy, and it continues to anchor its contemporary approach to economic security. From the export-oriented industrialization drive of the 1960s onward, South Korea pursued a mercantilist development model aimed at rapid catch-up with advanced economies. This model relied on active state guidance, protection and nurturing of strategic sectors, and close coordination with large industrial conglomerates.

The transition to democracy in the late 1980s shifted South Korea's industrial policy from a top-down, state-led mandate toward a more transparent system that balances corporate growth with public accountability and social welfare. This democratic shift decentralized economic power, forcing the government to move away from simply picking winners and toward fostering a resilient, innovation-based ecosystem that reflects broader national interests.

In the current context, industrial policy remains the primary means through which South Korea seeks to enhance economic security. However, its focus has shifted. Whereas earlier phases prioritized scale, export competitiveness, and sectoral upgrading, today's industrial policy increasingly targets **systemic resilience**, particularly in upstream inputs, critical technologies, and enabling components that underpin advanced manufacturing ecosystems. Strengthening technological depth and domestic capability is viewed not only as an economic objective, but also as a buffer against external pressure and supply disruption.

A Reactive but Adaptive Strategic Posture

A second defining feature of South Korea's economic security strategy is its **reactive character**, which stands in contrast to the more proactive, values-aligned approaches seen in **Australia** and **Finland**. Rather than pursuing pre-emptive coercion, South Korea has historically evolved its strategy as a direct response to specific instances of pressure from China and Japan, focusing on damage limitation and structural resilience. This has resulted in a **"dual-track"** system that reflects South Korea's unique constraints as a trade-dependent economy: it simultaneously fortifies domestic high-tech leadership while aggressively mitigating supply chain vulnerabilities to buffer against future external shocks.

This reactive posture was evident in Seoul's response to China's informal sanctions following the THAAD deployment and to Japan's 2019 export controls. In both cases, the government prioritized stabilization and adaptation, supporting affected firms, diversifying supply sources, and accelerating domestic capability-building rather than

retaliatory measures. Over time, these experiences reinforced the view that resilience, rather than retaliation, offers the most credible defense against economic coercion.

Importantly, reactivity has not meant passivity. Instead, it has encouraged **adaptive policy learning**, with each episode of disruption prompting institutional reform, legal reinforcement, and deeper coordination across government and industry.

Reducing Structural Supply Chain Vulnerabilities

Despite its strong manufacturing base and global export competitiveness, South Korea faces pronounced structural vulnerabilities in its supply chains. These stem from heavy reliance on external sources, often highly concentrated geographically, for raw materials, critical minerals, and specialized intermediate goods. Episodes such as the 2019 Japanese export controls and the 2021 Chinese urea restrictions made these dependencies visible and politically salient⁴⁶.

In response, South Korea has pursued a deliberate strategy of **vulnerability reduction**, combining diversification, selective localization, and targeted support for domestic upstream industries⁴⁷. The focus on materials, parts, and equipment (so-bu-jang) reflects an effort to secure control over choke points that could otherwise be exploited under conditions of geopolitical stress. This strategy is framed not as isolationism, but as risk management: reducing single-country dependence while maintaining participation in global production networks.

Linking Industrial Policy and Technological Sovereignty

A further evolution in South Korea's economic security thinking is the tighter coupling of industrial policy with technological innovation. Rather than treating technology as a by-product of industrial competitiveness, policymakers increasingly view **technological sovereignty** as a strategic asset in its own right⁴⁸.

This shift is evident in initiatives such as the designation of national strategic technologies, the Super Gap R&D strategy, and targeted programs to create globally dominant firms in critical upstream segments. By strengthening innovation capacity alongside supply chain resilience, South Korea seeks to move from vulnerability reduction toward **structural leverage**, positioning itself as an indispensable node within trusted global value chains.

Technology as Both Shield and Connector

Finally, advanced technology functions as both a defensive and cooperative instrument in South Korea's economic security strategy. Domestically, technological capability reduces exposure to coercion by limiting substitutability and dependence. Internationally, it enables deeper cooperation with trusted partners, most notably the

⁴⁶ Kim et al. 2021. "An analysis of South Korean industry's supply chain vulnerabilities and their ripple effects." November 18 (in Korean).

⁴⁷ The Supply Chain Stabilization Fund, established on September 5, 2024, introduced 5 trillion won in funding by having the Korea Exim Bank issue bonds guaranteed by the government. The government plans to expand this fund to 10 trillion won annually starting in 2025 (Ministry of Trade, Industry and Energy. 2024. Financial support guidelines for supply chain stabilization funds (in Korean).

⁴⁸ Relevant Ministries 2023. "Leading-Edge R&D Strategy for Three Core Technologies: Semiconductors, Displays, Next-Generation Batteries." April 6 (in Korean).

United States, in areas such as semiconductors, batteries, and emerging dual-use technologies.

Participation in plurilateral initiatives and technology partnerships allows South Korea to align domestic resilience objectives with allied supply chain restructuring. In this sense, technology serves as the bridge between national security priorities and international economic integration⁴⁹.

2.4.2 South Korea's Supply Chain Strategy: Institutions, Governance, and Instruments

South Korea's supply chain strategy translates its broader economic security objectives into a dense institutional and legal architecture designed to **identify vulnerabilities, coordinate responses, and stabilize critical flows** under conditions of uncertainty. Unlike more decentralized or incentive-led approaches, South Korea has opted for a **law-driven, state-coordinated model**, in which supply chain resilience is pursued through formal mandates, standing committees, and dedicated financial instruments.

At its core, this strategy reflects a belief that market mechanisms alone are insufficient to manage systemic risk in a geopolitically contested environment. Instead, the government has sought to embed supply chain governance within the central machinery of economic policymaking, elevating it to a national priority comparable to macroeconomic stability or industrial competitiveness.

Reforming the Legal and Institutional Foundation

A central pillar of South Korea's supply chain strategy is the construction of a comprehensive legal framework for economic security. Policymakers identified fragmented authority and weak statutory mandates as key sources of vulnerability during earlier crises. In response, South Korea enacted a series of interlocking laws that together provide the legal basis for state intervention, coordination, and support⁵⁰.

These include the three core supply chain laws collectively referred to as the Key Supply Chain Acts, which establish statutory authority for stabilizing critical supply chains, strengthening competitiveness in materials, parts, and equipment, and safeguarding access to strategic resources⁵¹. These are complemented by the Special Act on the Fostering of National Strategic Technologies and legislation protecting high-tech strategic industries.

Taken together, this legislative architecture enables a more **systematic and anticipatory approach** to supply chain governance. Rather than reacting through ad hoc measures, the government now operates within a standing legal framework that defines priorities, allocates responsibilities, and authorizes intervention before disruptions escalate into crises.

Early Warning Systems and Risk Detection

⁴⁹ Seungjoo Lee. 2025. "High technology and economic statecraft: the emergence of techno-economic statecraft in South Korea." *Business and Politics* 1-20. doi:10.1017/bap.2023.34.

⁵⁰ Ministry of Economy and Finance. 2022. Proposal for the Basic Law on Supply Chain Stabilization Support (in Korean).

⁵¹ South Korea's supply chain reforms in the 2020s were primarily driven by a realization that its "miracle" export economy was dangerously vulnerable to the weaponization of trade. While the 1960s–80s were about building capacity, the 2020s became about protecting it from external shocks. The Biden administration's 'friendshoring' policies, principally the CHIPS and Science Act, also influenced the government to seek reducing dependency on China.

Early identification of supply chain stress is a core operational objective of South Korea's strategy. To this end, the government has prioritized the development of a government-wide Early Warning System (EWS) capable of detecting emerging risks across thousands of items and multiple stages of production.

Previously, supply chain monitoring functions were dispersed across individual ministries and agencies, each operating their own information systems. Recent reforms have focused on integrating these capabilities into a unified framework that enables real-time information sharing and coordinated response. Inputs to the EWS include overseas market intelligence, customs clearance data, stockpiling information, procurement indicators, and mineral supply assessments, drawn from agencies such as the Ministry of Foreign Affairs, Korea Customs Service, the Public Procurement Service, the Korea Trade-Investment Promotion Agency, and the Korea Mine Rehabilitation and Mineral Resources Corporation.

The objective is not merely situational awareness, but **actionable foresight**. By identifying abnormal price movements, supply disruptions, or geopolitical signals at an early stage, authorities aim to activate targeted policy tools such as stock release, financing support, or diplomatic engagement before shortages cascade through the economy.

Centralized Governance and the “Control Tower” Model

South Korea's supply chain strategy is characterized by a high degree of centralization at the executive level. Recognizing that fragmented governance slowed responses during earlier disruptions, the government has restructured coordination mechanisms to create clear lines of authority and accountability.

At the apex of this system is the Supply Chain Stabilization Committee, established under the Framework Act on Supply Chains, which entered into force in June 2024. Chaired by the Minister of Economy and Finance, the committee functions as the central “control tower” for supply chain policy, coordinating actions across ministries and aligning stabilization measures with broader economic and fiscal objectives.

The committee oversees the designation of economic security items and services, sets strategic priorities, and deliberates on policy responses. In 2025, the scope of designated items was refined to focus on high-risk categories, including critical minerals, aerospace, defense-related goods, and essential public welfare items. On the services side, the definition was expanded beyond shipping and aviation to encompass the wider logistics ecosystem.

This governance structure reflects South Korea's preference for **hierarchical coordination** over network-based or voluntary models, ensuring that decisions can be taken rapidly under conditions of stress.

Financial Instruments: The Supply Chain Stabilization Fund

To complement regulatory and governance reforms, South Korea has deployed significant financial resources to support supply chain resilience. The Supply Chain Stabilization Fund, launched in September 2024, represents a central instrument in this effort.

Backed by government guarantees and administered through the Korea Export–Import Bank, the fund initially mobilized 5 trillion won, with plans to expand annual capacity to 10 trillion won. Its purpose is to support projects that enhance stability in four priority areas: advanced strategic industries, resource security, essential goods, and logistics infrastructure.

Rather than functioning as a general subsidy mechanism, the fund is explicitly risk-targeted. Preferential support is directed toward Tier-1 economic security items with high concentration risk or exposure to external disruption. Over time, the government has articulated quantitative goals for reducing dependency on single countries for key items, reflecting a shift from qualitative resilience rhetoric toward measurable diversification outcomes.

Public-private Coordination and Information Sharing

While South Korea's model is state-led, it increasingly recognizes the necessity of public-private cooperation. Supply chain risks often materialize at firm level, particularly among upstream suppliers and specialized SMEs. As a result, governance reforms have sought to expand structured engagement with industry, particularly in advanced technology sectors and the materials, parts, and equipment ecosystem.

Private-sector participation is encouraged through information sharing, joint risk assessment, and targeted support programs. However, compared to the Finnish model, public-private cooperation in South Korea remains more **directive than co-governed**, with the state retaining primary agenda-setting authority and firms responding within a defined policy framework.

Assessment

South Korea's supply chain strategy reflects a distinctive governance logic: resilience is pursued through **law, central coordination, and targeted financial mobilization**, rather than through voluntary institutionalized cooperation or market-led adjustment alone. This approach offers clear advantages in speed, clarity, and political visibility, particularly in a security environment marked by repeated shocks.

At the same time, it places significant demands on administrative capacity and risks rigidity if policy instruments are not continuously updated. As supply chains evolve and risks shift, the effectiveness of South Korea's model will depend on its ability to maintain flexibility within a highly formalized governance structure.

2.4.3 External Alignment and Trusted Supply Chains: The United States, Japan, China, and Multilateral Frameworks

South Korea's supply chain and economic security strategy is deeply shaped by its external environment. As a highly trade-dependent economy embedded in global manufacturing networks, South Korea cannot pursue resilience through domestic measures alone. Instead, it has sought to **externalize resilience** by aligning domestic capability-building with trusted international partnerships, while managing exposure to geopolitical risk through diversification and selective de-risking.

This external alignment does not follow a single doctrinal template. Rather, it reflects a pragmatic, interest-driven approach in which South Korea calibrates its posture toward

major partners based on sectoral exposure, technological position, and security considerations.

The United States: Anchor Partner for Advanced Industrial Supply Chains

The United States occupies a central position in South Korea's trusted supply chain strategy, particularly in advanced industries such as semiconductors, batteries, shipbuilding, and emerging dual-use technologies. Cooperation with the U.S. serves multiple functions simultaneously: it strengthens alliance ties, embeds South Korean firms in high-value production ecosystems, and reduces exposure to supply chain disruption linked to U.S.-China strategic competition.

During the Biden administration, South Korea actively aligned with U.S. reshoring and supply chain restructuring initiatives, particularly in response to the CHIPS and Science Act and incentives targeting advanced manufacturing. This alignment translated into a sharp increase in South Korean foreign direct investment in the United States, especially in semiconductor fabrication, battery production, and EV-related supply chains. From a South Korean perspective, these investments functioned less as simple market expansion than as **risk-hedging measures**, ensuring continued access to critical markets, technologies, and regulatory goodwill⁵².

While the language of "friendshoring" gained prominence during this period, South Korea's underlying strategy was more accurately characterised as **alliance-anchored diversification**. By deepening industrial integration with the United States, South Korea sought to secure its position within trusted supply chains for advanced industries, even at the cost of higher production expenses or trade imbalances.

The return of a second Trump administration has added complexity to this strategy. Renewed emphasis on reciprocal tariffs, trade balance concerns, and investment conditionality has forced South Korea to adapt once again. High-profile investment commitments announced in 2025 spanning shipbuilding, semiconductors, nuclear power, batteries, and bio-industries reflect Seoul's effort to preserve strategic alignment while navigating a more transactional U.S. trade posture. In this context, trusted supply chains are increasingly framed not as static alliances, but as negotiated arrangements requiring continuous political and economic management.

Japan: From Supply Chain Shock to Selective Normalization

Japan occupies a unique position in South Korea's economic security calculus. The 2019 Japanese export controls on semiconductor-related materials exposed South Korea's vulnerability to concentrated upstream dependencies and served as a catalytic shock for domestic supply chain reform.

In response, South Korea prioritized rapid localization and diversification in materials, parts, and equipment, reducing reliance on Japanese suppliers in several critical areas. This episode reinforced the government's determination to secure upstream resilience as a core component of economic security.

At the same time, recent years have seen a cautious normalization of bilateral relations, driven by shared concerns over regional security, technology competition, and supply

⁵² Last year, 43% of South Korea's overseas investment went to the United States, with "Korean intermediate goods" leading U.S. manufacturing." *Yonhap News*. November 10 (in Korean).

chain stability. While trust remains incomplete, pragmatic cooperation has resumed in selected areas, particularly where alignment with U.S.-led frameworks encourages coordination rather than rivalry. Japan thus illustrates how South Korea's trusted supply chain logic allows for **conditional re-engagement** once vulnerabilities have been addressed.

China: Managing Dependence Without Decoupling

China remains South Korea's largest trading partner and a critical node in its manufacturing ecosystem. At the same time, repeated experiences of economic coercion have fundamentally altered Seoul's risk perception. South Korea no longer views economic interdependence with China as politically neutral; instead, it treats concentrated dependence as a strategic liability requiring active management.

South Korea's approach toward China is therefore best described as **selective de-risking** rather than decoupling. The government has sought to reduce exposure in sensitive sectors, particularly those involving advanced technologies, strategic materials, or national security relevance, while maintaining commercial engagement in less sensitive areas.

Supply chain policy plays a central role in this strategy. Diversification of sourcing, investment in domestic upstream capabilities, and participation in trusted multilateral initiatives are designed to limit China's potential leverage without severing economic ties. This balancing act reflects both economic necessity and strategic caution, given South Korea's geographic proximity and security environment.

Multilateral and Plurilateral Frameworks

Beyond bilateral relationships, South Korea has increasingly leveraged multilateral and plurilateral frameworks to reinforce trusted supply chains. Participation in initiatives such as the Minerals Security Partnership supports diversification of critical mineral supply and aligns South Korea with like-minded economies seeking to reduce concentration risk.

Similarly, South Korea's engagement in trilateral cooperation with the United States and Japan, as well as broader technology and supply chain dialogues, reflects an effort to embed national resilience strategies within collective governance structures. These frameworks provide political cover, information-sharing channels, and coordination mechanisms that reduce the costs of unilateral action.

Assessment

South Korea's external alignment strategy underscores a central feature of its economic security approach: resilience is pursued through **strategic embedding rather than insulation**. Trusted supply chains are built by anchoring domestic capability-building within alliance frameworks, while selectively reducing exposure to dependencies that cannot be governed through trust or reciprocity.

At the same time, South Korea's experience highlights the fluidity of trusted supply chains. Political transitions, trade disputes, and shifting alliance dynamics require constant recalibration. For South Korea, the challenge is not only to align with trusted

partners, but to maintain strategic flexibility within an increasingly politicised global economy.

2.4.4 Public-Private Cooperation and Defence-Industrial Resilience in South Korea

Public-private cooperation occupies a central place in South Korea's economic security architecture, particularly at the intersection of defence, advanced technology, and industrial policy. Unlike Finland's institutionally routinised, trust-based model or Australia's incentive-driven, alliance-integrated approach, South Korea's system is best characterised as **state-orchestrated and industry-led**, with strong executive coordination and an explicit focus on scale, speed, and global competitiveness.

This model reflects South Korea's strategic environment. The persistent threat posed by North Korea, combined with exposure to great-power competition and economic coercion, has long prevented a strict separation between security policy and industrial development. As a result, defence-industrial policy is treated not as a niche sectoral concern, but as a core component of national resilience and economic strategy.

Governance Logic: From Procurement State to Strategic Orchestrator

At the heart of South Korea's public-private cooperation model lies a strong central state that actively shapes industrial outcomes while relying on private firms for execution and innovation. This governance logic is often described domestically as **"government-led, private-driven"**.

The transformation of defense governance illustrates this shift. The Defence Acquisition Program Administration (DAPA), once primarily a procurement authority, has evolved into a strategic industrial coordinator. Under the Defence Innovation 4.0 initiative, DAPA now plays a central role in accelerating capability development, integrating commercial technologies into military platforms, and reducing the time lag between innovation and deployment⁵³.

Crucially, regulatory reforms have altered the risk calculus for private firms. Companies participating in defense-related R&D are now permitted to retain intellectual property rights for jointly developed technologies, and "honorable failure" provisions limit penalties for unsuccessful high-risk projects. This effectively reframes defense innovation as a venture-style activity, encouraging firms to pursue asymmetric and dual-use technologies without existential commercial risk.

Compared with Australia's ASCA model, South Korea's approach is more centralised and directive. Compared with Finland's governance-by-trust architecture, it relies more heavily on formal authority, executive coordination, and strategic prioritization.

Industrial Structure: National Champions and Scale Effects

South Korea's defence-industrial ecosystem is dominated by a small number of large conglomerates—most notably Hanwha, Korea Aerospace Industries, LIG Nex1, and Hyundai Rotem. These firms function as national champions, combining defense

⁵³ Defense Acquisition Program Administration. n.d. "DAPA's Founding Background and Role." DAPA. Accessed December 30, 2025. https://www.dapa.go.kr/dapa_en/index.do?menuSeq=3470

production with broader industrial capabilities in aerospace, electronics, shipbuilding, and advanced manufacturing⁵⁴.

Public-private cooperation in this context is asymmetrical. The state provides strategic direction, diplomatic backing, and financial instruments, while large firms deliver scale, speed, and export capacity. Smaller firms and SMEs play supporting roles, often integrated into supply chains through tiered subcontracting rather than direct strategic partnership.

This structure enables rapid mobilization and global competitiveness but creates vulnerabilities at lower tiers of the supply chain, where dependence on imported materials and components remains high. As in Australia, resilience at the prime-contractor level does not automatically translate into resilience at Tier 2 and Tier 3 levels.

Defense Exports as a Resilience Instrument

A distinctive feature of South Korea's model is the explicit use of defense exports as a tool of economic security and industrial resilience. Rather than treating exports as a by-product of domestic capability, the government actively promotes them as a stabilizing force for the defense-industrial base.

This is operationalized through a **whole-of-government export strategy**, combining diplomatic engagement, industrial coordination, and state-backed finance. Institutions such as the Export-Import Bank of Korea and the Korea Trade Insurance Corporation provide credit guarantees and insurance that enable large-scale defense deals, most notably with Poland, to proceed despite liquidity constraints on the buyer side⁵⁵.

These “package deal” exports typically include not only equipment delivery, but also technology transfer, training, and local production facilities. From an economic security perspective, this model supports continuous production runs, workforce retention, and learning-by-doing, reducing vulnerability to demand shocks and reinforcing South Korea's position in trusted defense supply chains.

Emerging Domains and Blurring Boundaries

As in Australia and Finland, the boundary between civilian and military innovation in South Korea is increasingly blurred. Public-private cooperation now extends deeply into emerging domains such as artificial intelligence, autonomous systems, space, cyber, and quantum technologies.

The establishment of the Defence AI Center reflects this trend, coordinating with private technology firms to integrate autonomy and data-driven capabilities into platforms such as the KF-21 fighter and unmanned systems. Similarly, the Korea AeroSpace Administration promotes a private-led “New Space” ecosystem by transferring state-developed launch technologies to commercial actors.

⁵⁴ The Korea Herald. 2024. "Korea's four major defense companies boost revenues by 31%." *The Korea Herald*. Accessed December 30, 2025. <https://www.koreaherald.com/article/10628008>.

⁵⁵ The Korea Herald. 2024

These initiatives strengthen South Korea's technological edge but also increase reliance on complex, globally distributed supply chains for critical inputs, particularly advanced semiconductors and critical minerals.

Persistent Vulnerabilities and Friction Points

Despite its strengths, South Korea's public-private cooperation model faces several structural challenges.

First, upstream dependency remains significant. South Korea's advanced manufacturing ecosystem is highly dependent on imported critical minerals and specialized equipment. The Supply Chain Stabilization Fund and related diversification efforts are designed to mitigate this risk, but results will materialize only gradually.

Second, cybersecurity cooperation remains uneven. While information-sharing platforms exist, many private firms, especially SMEs, remain reluctant to share threat data due to concerns about regulatory scrutiny or liability. This creates a persistent gap between policy ambition and operational resilience.

Third, the concentration of capability in large conglomerates creates a resilience asymmetry. National champions are well positioned to absorb compliance costs, geopolitical risk, and supply disruptions; smaller firms are not. This mirrors challenges observed in Australia but is more pronounced given South Korea's scale-driven industrial structure.

Assessment

South Korea's public-private cooperation model reflects a strategic choice to prioritize **speed, scale, and technological leverage** in a high-threat environment. Trusted supply chains are built less through voluntary institutionalized trust (as in Finland) and less through alliance-embedded incentives (as in Australia), and more through **state-orchestrated industrial mobilization** aligned with national security objectives.

This approach has delivered rapid capability development, export success, and growing technological autonomy. At the same time, it places heavy demands on governance capacity and risks overlooking fragilities below the level of national champions.

The South Korean case demonstrates that trusted supply chains can be constructed through strong state coordination and industrial power, but that sustaining resilience across the full supply chain requires continued attention to upstream dependencies, SME integration, and information-sharing incentives.

Chapter 3: Corporate Practices, Perceptions, and Constraints in Trusted Supply Chains

3.1 Introduction

As geopolitical competition increasingly shapes global trade, technology flows, and industrial policy, firms operating in strategic and dual-use sectors are being drawn more directly into questions of national and allied economic security. Governments may set the policy direction, but the effectiveness of trusted supply chains ultimately

depends on how companies perceive risk, allocate resources, and adapt operational practices. This chapter examines how firms in three key U.S. partner countries—Australia, Finland, and South Korea—understand and respond to this evolving environment.

The analysis is based on a structured survey conducted between **15 September and 15 December 2025**, targeting companies active in **dual-use technologies**, including AI, drone technologies, and advanced sensors. These sectors sit at the intersection of civilian innovation and defense capability and are therefore particularly exposed to geopolitical risk, export controls, intellectual property concerns, and supply chain disruption.

By focusing on Australia, Finland, and South Korea, the survey captures corporate perspectives across three distinct but strategically relevant contexts:

- a highly allied Indo-Pacific defense economy with deep integration into U.S. supply chains;
- a frontline European security state with strong technological capabilities and exposure to Russia-related risk; and
- an advanced East Asian manufacturing economy shaped by direct experience of economic coercion.

The objective of the survey was not to generate statistically representative results, but to surface **how firms interpret economic security in practice**, how they manage supply chain risk, and where frictions arise between policy ambitions and corporate realities.

3.2 Survey Scope, Structure, and Respondent Profile

Survey Design and Thematic Areas

The survey employed a mixed-methods design, combining **multiple-choice, scaled**, and **open-text** questions. It covered six thematic areas:

1. **Company profile and operational context**, including location, sector, size, and level of involvement in dual-use technologies.
2. **Supply chain resilience practices**, including risk assessment, diversification, visibility, crisis management, cybersecurity, and obsolescence mitigation.
3. **Awareness of geopolitical risk and trusted supply chain concepts**, including understanding of economic security and “friendshoring.”
4. **Perceptions of government policy and support**, including awareness of national and U.S.-linked initiatives.
5. **International collaboration**, focusing on opportunities and barriers to cooperation with U.S. partners.
6. **Dual-use technology-specific considerations** (optional), including security by design, talent, ethics, and innovation management.

In total, the survey consisted of **24 structured questions** and **5 open-text questions**.

Target Population and Sample Characteristics

The survey was distributed to **122 companies** headquartered in Finland, Australia, and South Korea. The final sample consisted of **27 respondents**, reflecting the challenges of engaging firms on sensitive security-related topics.

Key characteristics of the respondent pool include:

- **Country distribution:**
 - Finland: 66%
 - South Korea: 17%
 - Australia: 17%
- **Industry sectors:**
 - ICT: 50%
 - Defense: 33%
 - Manufacturing: 17%
- **Company size:**
 - Large enterprises (250+ employees): 50%
 - Remaining respondents span small and medium-sized firms
- **Technology integration:**
 - Extensive/core involvement: 33%
 - Moderate involvement: 33%
 - Limited/exploratory involvement: 17%
- **Market reach:**
 - Large firms predominantly operate globally
 - Smaller firms focus on domestic or regional markets

Respondents included technology developers, manufacturers, system integrators, and significant end-users, providing insight across different positions within strategic supply chains.

3.3 Methodological Caveats

The findings presented in this chapter should be read as **exploratory and indicative**, rather than statistically representative. Several limitations are particularly important:

- **Small sample size and country skew:** Finnish firms are overrepresented relative to Australian and South Korean respondents.

- **Selection bias:** The survey targeted firms already active in high-risk dual-use sectors, likely increasing awareness of geopolitical issues relative to the broader corporate population.
- **Sectoral focus:** Results reflect conditions in technology-intensive industries and may not generalize to lower-tech or purely commercial sectors.

To mitigate these constraints, survey findings are interpreted alongside:

- qualitative responses,
- expert interviews and practitioner insights, and
- the country-level policy analysis presented in Chapter 2.

The value of the survey lies less in precise quantification and more in revealing **how firms conceptualize economic security and trusted supply chains from the ground up.**

3.4 Summary of Key Findings

Across countries and sectors, several consistent patterns emerge:

Geopolitical Risk Is Now Structurally Embedded in Business Strategy

Respondents report that geopolitical shocks—most notably the Russia-Ukraine war—have had a **significant and lasting impact** on supply chain strategies. Risk is no longer treated as episodic but as a persistent operating condition.

Resilience Is Pursued Through Technical and Contractual Means

Firms emphasize **modular design, inventory management, and long-term customer contracts** as tools to manage obsolescence and supply uncertainty. These measures allow technical adaptation without full supplier replacement.

Economic Security Is Defined Operationally, Not Ideologically

Companies tend to define economic security as the ability to maintain **continuous operations, R&D, and production** under conditions of geopolitical stress. This definition is closely linked to:

- access to cutting-edge technology,
- stable manufacturing capacity, and
- predictable regulatory environments.

Supply Chain Visibility Remains Limited

Most firms report only **moderate visibility beyond Tier-1 suppliers**. Finnish firms report particularly low upstream visibility, while the South Korean manufacturing respondent reports higher visibility, likely reflecting more vertically integrated industrial structures.

Intellectual Property and Data Security Are Central Barriers

Concerns over internet protocol (IP) protection and data security are consistently cited as the main obstacles to deeper international collaboration. Firms express a strong preference for **government-backed assurance mechanisms** rather than purely contractual solutions.

Strong Interest in Allied Frameworks

Awareness of frameworks such as **AUKUS**, **SOSA**, and **NATO-linked mechanisms** is high, and these are widely seen as potential vehicles for trusted supply chain integration—though detailed understanding varies.

3.5 Supply Chain Resilience in Practice

Risk Assessment and Governance

Most firms conduct some form of supply chain risk assessment, but frequency and depth vary significantly:

- Large firms tend to conduct assessments annually or continuously.
- Smaller ICT firms report more ad hoc or limited practices.

Regulatory exposure is uneven: approximately **60% of respondents** report being subject to formal supply chain or security-related legislation, particularly in Finland and South Korea.

Managing Obsolescence and Availability

To address rapid technological change, firms rely on:

- modular system architectures,
- long-term procurement planning,
- technical review cycles led by senior engineers or “technical fellows.”

These practices allow substitution of components without redesigning entire systems, reducing vulnerability to single-point failures.

3.6 Trusted Supply Chains and International Collaboration

Understanding of “Friendshoring” and Trusted Partners

Although terminology varies, firms across all three countries converge on a similar logic:

economic security is achieved by **strengthening cooperation with trusted partners**, rather than by geographic reshoring alone.

South Korean respondents emphasize operational continuity under coercive pressure. Australian respondents link economic security to warfighter protection and access to advanced R&D.

Finnish respondents highlight regulatory predictability and alliance-based trust.

Barriers to Deeper Cooperation

Despite interest in allied collaboration, firms identify persistent obstacles:

- uncertainty around export controls,
- fear of IP leakage,
- lack of secure environments for joint R&D.

Respondents repeatedly suggest that **license-free or pre-cleared environments among trusted allies** would materially reduce these barriers.

3.7 Insights from Open-Ended Responses

The qualitative responses reinforce three overarching themes:

1. **Firms increasingly see themselves as strategic assets**, not merely commercial actors, particularly in defense-linked sectors.
2. **Resilience strategies are proactive but policy-dependent**: companies can manage technical risk internally, but require government-backed frameworks for cross-border trust.
3. **Trusted partnerships matter more than location**: resilience is tied to whom firms cooperate with, not simply where production occurs.

One South Korean respondent described economic security as the resilience of the firm's entire operational ecosystem, sustained through government contracts and alignment with allied defence forces. Others stressed the importance of secure, rule-based environments that allow suppliers to collaborate without excessive regulatory friction.

3.8 Implications for Trusted Supply Chain Policy

The survey suggests a consistent gap between **policy ambition** and **corporate execution capacity**. Firms are broadly aligned with the logic of trusted supply chains but face practical constraints related to cost, compliance, and uncertainty.

Three implications stand out:

- **Visibility beyond Tier-1 remains a weak link**, particularly for SMEs.
- **Security and resilience impose real cost premiums**, which firms cannot always absorb without support.
- **Trust must be institutionalized**, not assumed—through predictable rules, shared standards, and credible assurance mechanisms.

These findings reinforce the country-level analysis in Chapter 2: trusted supply chains are not achieved through declarations alone, but through sustained public-private coordination that makes security-compatible behaviour commercially viable.

Chapter 4: Case Study Vignettes – Corporate Realities

While Chapters 2 and 3 examined national policy frameworks and broad corporate perceptions of economic security, this chapter shifts the focus to **operational reality**. Through targeted case study vignettes, it illustrates how firms experience and navigate the frictions that arise when high-level economic security objectives meet commercial, legal, and technical constraints.

The vignettes presented here are not intended to be statistically representative or exhaustive. Instead, they serve as **illustrative deep dives**, grounded in interviews, expert assessments, and institutional evidence, to surface recurring structural tensions that are often obscured in policy design and survey responses. Together, they demonstrate how trusted supply chains are shaped not only by strategic intent, but by legacy obligations, regulatory boundaries, cost structures, and firm-level risk trade-offs.

4.1 Case Study Vignette 1: The “Fast Follower” Dilemma – Balancing Sovereignty with Commercial Survival in South Korea

This vignette examines the strategic posture of a **major South Korean automotive conglomerate** that is transitioning from traditional vehicle manufacturing toward a broader role as a comprehensive mobility provider, with expanding interests in **urban air mobility (UAM), robotics, and autonomous systems**. The firm exemplifies the structural tension between government-led economic security objectives and the commercial realities faced by globally integrated, legacy manufacturing firms.

The “Tier-1 Wall” and Legislative Friction

The company reports high visibility and control over its Tier-1 suppliers, but a **systemic opacity beyond this level**, particularly with respect to Tier-2 and Tier-3 providers. This visibility gap is not merely technical or informational; it is reinforced by domestic regulation. The firm identifies South Korea’s *Fair Transactions in Subcontracting Act* as a material constraint, noting that direct audits or intervention in lower-tier supplier operations can create legal exposure related to unfair interference.

As a result, the company must rely heavily on information filtered through Tier-1 suppliers, limiting its ability to directly assess upstream vulnerabilities—especially in areas such as **critical minerals (e.g. cobalt, tungsten)** and specialized components. This creates a paradox: while the state increasingly demands deeper supply chain transparency for economic security reasons, existing fair-trade legislation constrains the mechanisms through which such transparency can be achieved. The firm has therefore advocated for targeted legislative clarification or exemptions to reconcile security-driven transparency requirements with competition law.

Decoupling Inertia: Legacy Obligations versus Geopolitical Pressure

The vignette highlights the **practical limits of rapid decoupling from China**. Despite a strategic intent to diversify sourcing toward Southeast Asia and other regions, the company reports that its exposure to Chinese suppliers has, in some cases, **increased rather than declined**.

A key driver is the automotive industry's **long-term after-sales service obligation**, typically extending up to ten years. Components for vehicles already in circulation must remain available, making abrupt supplier disengagement commercially and legally untenable. In parallel, the firm notes that for certain industrial inputs—such as molds, dies, and precision tooling—Chinese suppliers continue to offer advanced capabilities that are difficult to replace quickly without incurring quality or timeline risks.

These dynamics illustrate how economic security objectives collide with **path dependence** created by installed product bases, consumer obligations, and deeply embedded industrial ecosystems.

The Real Cost of “Friendshoring”

The company provides a blunt assessment of the costs associated with relocating production to the United States. Labor costs are estimated to be roughly **three times higher** than in South Korea, while environmental and permitting constraints complicate the establishment of essential manufacturing processes such as coating and painting facilities.

In addition, the firm faces a complex regulatory landscape shaped by overlapping pressures: U.S. protectionist measures on the one hand, and the European Union's Corporate Sustainability Due Diligence Directive on the other. Rather than full reshoring to the United States or re-concentration in Korea, the company is pursuing a strategy of **regionalization**, notably by establishing supply chain hubs in **Eastern Europe**. This approach is viewed as a second-best solution that balances geopolitical alignment, cost control, and regulatory compliance.

Key Insight

This vignette illustrates that for globally embedded firms, trusted supply chains are often constrained less by strategic intent than by **legacy commitments, legal structures, and cost realities**. Economic security objectives may be recognized and accepted at the corporate level, but their implementation is mediated by commercial survival imperatives and institutional frictions that limit the speed and scope of adjustment.

4.2 Case Study Vignette 2: Australian Defense Supply Chain Dynamics – A System-Level Perspective

This vignette does not focus on a single firm but presents a **policy-grounded narrative synthesis** drawn from parliamentary committee evidence, industry testimony, and professional experience within the Australian defense procurement ecosystem. It reflects how defense authorities and major prime contractors collectively understand and manage supply chain risk in practice.

Critical Vulnerabilities and Chokepoints

Across testimony and expert assessments, advanced electronics, specialized munitions components, and secure software systems consistently emerge as **primary vulnerabilities**. These dependencies are characterized by limited numbers of qualified

suppliers, long certification timelines, and stringent security requirements. Disruptions in any of these areas can halt capability delivery for months.

Beyond physical inputs, officials emphasize the importance of **horizontal dependencies** – secure ICT networks, personnel security clearances, and export control compliance systems. Interruptions in these enabling functions can stall activity across entire programs, even when material supply remains intact.

Visibility Beyond Tier-1

Supply chain visibility remains strongest at the Tier-1 level and declines rapidly further upstream. Historically, both Defense and primes relied heavily on self-reporting by contractors. Recent reforms under the Defense Industry Development Strategy have pushed toward more data-driven approaches, including tools such as the **Supply Network Analysis Program**.

In practice, mapping deeper tiers involves a combination of contractual disclosure obligations, third-party analytics, and targeted “deep dives” into high-risk inputs such as semiconductors and rare earths. This is not a one-off exercise but a continuous process, supplemented by ongoing monitoring through mechanisms like the Defence Industry Security Program.

Preventing Diversion to Adversary Systems

Concerns about Western components appearing in adversary weapon systems are addressed through a layered control regime. This includes strict adherence to U.S. and multilateral export control regimes, contractual prohibitions on re-export, end-user certification, automated sanctions screening, and audit rights over intermediaries.

While these controls are considered robust, industry witnesses acknowledge that **grey-market leakage** remains a persistent risk. This has reinforced the view that supply chain risk management must increasingly incorporate intelligence-led assessments rather than rely solely on formal compliance.

Defining “Trusted” versus “Risky” Suppliers

In practice, suppliers are classified not through formal labels but through **jurisdictional and compliance-based heuristics**. Trusted suppliers are typically located in like-minded jurisdictions—such as Five Eyes, NATO, or close Indo-Pacific partners—where legal protections, cybersecurity standards, and export control alignment are strong.

“Necessary but risky” suppliers may be tolerated for non-critical items when alternatives do not exist, but are subject to heightened monitoring and contingency planning. The strategic objective is to progressively shift toward suppliers with demonstrable cyber maturity and reliable export control compliance.

The Role of the GSC Program

Within this ecosystem, the GSC Program is widely viewed as a critical enabler. Rather than treating Australian industry primarily through local content requirements, the program incentivizes primes to integrate Australian SMEs into **long-term global production programs**.

By co-funding dedicated teams within primes to identify and qualify Australian suppliers, the program lowers barriers to entry and provides SMEs with a credible export pipeline. This, in turn, justifies investments in cybersecurity, quality systems, and compliance that would otherwise be difficult to sustain on the basis of domestic demand alone.

Desired Non-Financial Interventions

Industry and Defense actors consistently highlight the importance of **non-financial government support**. From the Australian side, this includes intelligence-informed risk guidance and streamlined approvals across overlapping security and industry programs. From the U.S. side, greater predictability in export controls—particularly International Traffic in Arms Regulations (ITAR)—and enhanced data-sharing on supply chain risk signals are seen as critical to reducing friction in trusted supply chain integration.

Key Insight and takeaway

The Australian case illustrates how trusted supply chains are constructed through **incremental, system-level coordination** rather than through wholesale restructuring. While policy intent is clear, operational reality is shaped by chokepoints, compliance burdens, and the uneven distribution of capability and risk across the supply chain.

4.3 Case Study Vignette 3: Finnish Dual-Use Firms at the Economic Security-Readiness Interface

Unlike the preceding vignettes, which focus on firm- or system-level dynamics, this vignette captures ecosystem-level patterns observed across multiple Finnish dual-use SMEs operating within NATO-facing innovation environments. As such, it synthesizes recurring firm-level patterns observed among Finnish defense-adjacent and dual-use companies operating in Finland's Digital Defense Ecosystem (DDE). Rather than describing a single enterprise, it captures ecosystem-level dynamics encountered by technology providers spanning cyber, Intelligence, Surveillance, and Reconnaissance (ISR)/data analytics, space-enabled services, secure connectivity, autonomy, sensors, and mission-critical software.

While this vignette draws primarily on Finnish ecosystem experience, DDE member companies operate across the wider NATO market, including the United States. From their perspective, the dynamics described here are not uniquely Finnish: the same tensions recur across NATO member states, reflecting a broader system-level pattern rather than a national exception.

The focus of this vignette is practical: how economic security objectives translate into operational constraints, and how strategic dependency management is experienced inside product development, procurement pathways, compliance processes, and scaling decisions. The vignette is structured around three themes: (1) how dependencies materialize in practice, (2) where policy intent and company realities diverge, and (3) what these frictions imply for firms operating in dual-use or strategically sensitive environments.

This section concludes with three core recommendations aimed at translating the vignette's insights into practice.

1) Strategic Dependencies in Practice: How Economic Security Materializes Inside Firms

- *Component chokepoints and the “small-N supplier” problem:* Across the ecosystem, strategic dependency is often most visible in narrow, high-criticality component categories where supplier diversity is structurally limited. Even when a system is modular, certain inputs—advanced sensors, specialized RF components, secure elements, optical assemblies, ruggedized connectors, and high-assurance electronics—remain tied to globally concentrated production and slow qualification cycles. For SMEs, the vulnerability is not only supply risk but **predictability risk**: uncertain lead times cascade into missed integration windows, delayed fielding, and reputational damage. Dependency becomes a credibility variable: the ability to deliver is shaped as much by upstream allocation and certification timelines as by the firm’s own engineering performance.
- *Software, licensing, and update sovereignty as operational dependency:* For many dual-use firms, dependency is now software-defined. In cloud-enabled ISR, analytics, secure data exchange, and digital command-and-control enablers, the critical sovereignty question is not “where the hardware was assembled,” but who controls the system’s lifecycle. Platform reliance (cloud ecosystems, data services, compute environments), software supply chain integrity (libraries, continuous integration and continuous delivery toolchains), and the ability to patch and reconfigure under crisis conditions have become central. A system may be physically produced in Europe yet remain dependent on non-European permissions, licenses, or vendor-controlled update pipelines. In strategically sensitive contexts, **update rights and cryptographic agility**—the capacity to change core cryptographic algorithms and configurations without external permissions—form one practical boundary of technological sovereignty.
- *Exportability and classification ambiguity as day-to-day constraints:* Economic security enters daily operations through export controls, sanctions screening, end-user restrictions, and **shifting interpretations of dual-use classification**. For firms, these are not static obligations but variables that shape market strategy, product demonstrations, and customer eligibility. Compliance is experienced less as a one-time hurdle and more as an ongoing cost structure: **“comply continuously”** rather than “comply once.” The volatility of the geopolitical environment amplifies this effect. A solution that is technically deployable can become commercially constrained due to regulatory uncertainty, customer-specific security interpretations, or changing risk thresholds tied to partner jurisdictions.

2) Policy-Reality Misalignment: Where Guidelines and Firm-Level Constraints Diverge

- *“Reduce dependencies” versus mixed-origin technology reality:* Economic security agendas increasingly favor reduced reliance on non-European inputs, yet firms operate within globalized technology stacks. Even when companies prefer European sourcing, constraints persist: European alternatives may not exist for certain niche components; qualification timelines can be incompatible with urgent delivery windows; and cost escalation can undermine competitiveness in export markets. This creates an operational contradiction for dual-use innovators: **deliver rapidly and restructure supply chains simultaneously**. At SME scale, these objectives often compete unless transition

mechanisms exist that explicitly fund redesign, qualification, and supplier replacement efforts while protecting delivery schedules.

- *Expanding compliance layers versus SME absorption capacity:* Companies recognize the legitimacy of security requirements, but the cumulative compliance stack is growing faster than SME capacity. Export controls, cyber maturity expectations, origin disclosure, supplier assurance, data governance, and security-specific contractual obligations increasingly operate in parallel. The effect is not simply administrative burden; it is competitive distortion. **Time spent meeting overlapping governance demands is time not spent on shipping, testing, fielding, and iterating.** The ability to scale becomes partly determined by compliance bandwidth rather than technical merit – a dynamic that favors incumbents and risks leaving innovative SMEs stuck as subcontractors rather than prime-capability providers.
- *Strategic autonomy as consensus goal – but not yet an operational model:* Strategic autonomy is broadly accepted as a guiding direction, yet it becomes actionable only when translated into prioritized criteria: which capability layers require sovereign control, which dependencies are acceptable, and which are mission-critical. **Without such prioritization, “autonomy” risks functioning as a slogan rather than a decision tool** – leaving firms to guess the long-term acceptability of supply chain choices, platform dependencies, and partnership models. For ecosystem companies, predictability is the central requirement: they can align with demanding standards if the standards are stable and clearly scoped.

3) Implications for Dual-Use and Sensitive-Tech Firms: What These Frictions Produce

- *The dual-use paradox: move fast, operate as “high-risk”:* Dual-use firms are increasingly treated as engines of speed while simultaneously regulated as potential security risk carriers. This produces **a two-track competition**. First, firms must deliver capability performance: integration, reliability, and deployability. Second, they must deliver trust performance: provenance, lifecycle control, compliance credibility, and resilience under crisis conditions. The second track is becoming decisive for market access. In practice, innovation is necessary but insufficient; the supplier itself must be governable, auditable, and reliable under disrupted supply and elevated threat environments.
- *Lifecycle control and modifiability as strategic differentiators:* In sensitive defense environments, the critical differentiator increasingly becomes freedom to operate across the lifecycle: independent modifiability, secure update pipelines, cryptographic agility, and the ability to sustain performance without external restrictions. This shifts competition from “best feature set” toward “best control of the operational lifecycle.” **Architecture and governance choices—build systems, signing practices, configuration authority, and secure update mechanisms—become strategic attributes**, not merely engineering details. Firms that can demonstrate sovereign lifecycle control are better positioned to compete for programs where readiness requirements and security constraints converge.

- *A rising “trust premium” in expanding markets:* The European defense market is expanding, but access is increasingly mediated by trust signals: transparent ownership, predictable compliance, resilient delivery pipelines, and demonstrable security-of-supply preparedness. This produces a trust premium that shapes who can scale. For Finnish ecosystem firms, the opportunity is substantial, but the pathway is conditional: **success depends not only on innovation speed but also on the ability to operate within an economic security logic that treats suppliers as part of the defense system’s resilience.**

Key insights

This vignette highlights that for dual-use and strategically sensitive firms, economic security is lived reality rather than abstract doctrine. It manifests through component chokepoints, limited upstream visibility, software and update dependencies, expanding compliance demands, and procurement mechanisms that do not yet consistently convert urgency into predictable scale demand.

Moreover, key finding of this vignette is that a central challenge is operational alignment, i.e. translating strategic intent into practice. To help achieve this, three actions are needed:

1. First, strategic urgency must be converted into **procurement predictability** through contracting mechanisms and multi-year demand commitments that allow firms, especially SMEs, to invest and scale with confidence.
2. Second, “strategic autonomy” must be made **actionable and prioritized**, with sovereignty requirements clearly defined in tiered form and centered on the layers that matter most in practice, e.g.: lifecycle control, update rights, modifiability, and cryptographic agility.
3. Third, Europe needs **transition mechanisms** that enable companies to restructure dependencies without sacrificing deliverability. Thus can be, for example, funding redesign and re-qualification, supporting second-source validation, and reducing compliance friction through reusable trust and assurance structures (which must be clear and standardized).

In combination, these steps turn economic security from an abstract doctrine into a practical industrial model, the outcome of which is strengthened readiness and the ecosystem’s capacity to innovate and deliver under pressure.

Taken together, the three vignettes demonstrate that trusted supply chains are not implemented on a blank slate. They are negotiated within environments shaped by legacy obligations, regulatory constraints, cost asymmetries, and imperfect information. These realities do not invalidate economic security objectives—but they condition how, and how far, firms can move in response.

These empirical frictions form the basis for the cross-cutting analysis in **Chapter 5**, which examines how such tensions recur across national contexts and what they imply for the design of sustainable public-private cooperation on trusted supply chains.

Chapter 5: Governing Trusted Supply Chains – Frictions, Trade-Offs, and Public-private Coordination

The preceding chapters demonstrate that trusted supply chains are no longer a marginal concern at the intersection of trade and security. They have become a central organizing principle for economic security policy among U.S. partners and a defining constraint shaping corporate strategy in dual-use and defense-adjacent sectors. Yet the case studies and survey evidence also show that trust cannot be legislated into existence, nor can it be assumed to flow automatically from political alignment.

This chapter synthesizes the findings from the national frameworks (Chapter 2), corporate survey results (Chapter 3), and firm-level vignettes (Chapter 4) to identify the **core frictions and trade-offs** that arise when governments seek to operationalize trusted supply chains through the private sector. Rather than treating these frictions as policy failures, the analysis treats them as **structural features** of contemporary geoeconomic governance that must be managed through sustained public-private coordination.

The central argument is that trusted supply chains function as a **governance problem** rather than a purely technical or locational one. Their durability depends on how effectively governments and firms align incentives, information flows, and compliance expectations under conditions of geopolitical uncertainty.

5.1 Trusted Supply Chains as a Governance Challenge

Across all three country cases, trusted supply chains are framed as an alternative to both unfettered globalization and inward-looking self-sufficiency. Governments do not seek to dismantle global markets, but to **restructure interdependence** in ways that reduce exposure to coercion, disruption, and strategic surprise. Firms, for their part, largely accept this logic—but only to the extent that it remains compatible with commercial viability, legal obligations, and long-term competitiveness.

This creates a fundamental governance tension. Economic security policies increasingly rely on private actors to implement objectives that serve collective security goals, such as export controls, supply continuity, and infrastructure protection. At the same time, firms remain accountable to shareholders, customers, and contractual obligations that often pull in different directions.

The empirical cases illustrate that trusted supply chains do not emerge from declarations of alignment alone. They are shaped by:

- regulatory clarity and predictability;
- the distribution of compliance costs across the supply chain;
- access to credible information about risk;
- and the presence of tangible incentives for participation.

Where these conditions are misaligned, trust becomes fragile, and firms revert to defensive or minimalist compliance strategies rather than internalizing security objectives into core business planning.

5.2 Visibility as the Persistent Bottleneck

One of the most consistent findings across the survey data and case vignettes is the **visibility gap beyond Tier-1 suppliers**. Governments increasingly expect firms to map and manage upstream dependencies, yet firms often lack both the legal authority and practical tools to do so.

The South Korean vignette illustrates how competition and subcontracting law can actively constrain upstream audits, even as security policy demands greater transparency. In Australia, Defense and primes have made progress through contractual and analytical tools, but mapping remains partial and resource-intensive. Finnish institutions benefit from deeper systemic visibility, yet even there, Tier-2 and Tier-3 dependencies present persistent challenges—particularly among SMEs.

This gap matters because systemic vulnerability is rarely concentrated at the top of the supply chain. Critical dependencies often lie in specialised inputs, niche processing capabilities, or single-point service providers several tiers upstream. Without credible visibility, trusted supply chain strategies risk reinforcing resilience at the prime level while leaving deeper fragilities unaddressed.

The implication is not that full transparency is achievable or desirable in all cases, but that **expectations around visibility must be aligned with legal frameworks, firm capacity, and proportionality**.

5.3 The Cost and Distribution of the “Security Premium”

Trusted supply chains are not cost-neutral. Across all three cases, firms absorb what can be described as a **security or resilience premium**: higher input costs, redundancy investments, compliance overhead, and opportunity costs associated with constrained market access.

Crucially, these costs are **unevenly distributed**. Large primes and national champions are generally able to absorb them through scale, pricing power, or government support. SMEs—often critical Tier-2 and Tier-3 suppliers—face proportionally higher burdens, particularly in areas such as cybersecurity, export control compliance, and continuity planning.

The Australian and Finnish cases show different mitigation strategies: Australia emphasizes export pipelines and capability uplift through integration into allied supply chains, while Finland relies more on institutionalized trust, early warning, and informational advantages. South Korea, by contrast, addresses cost asymmetries through centralized finance and industrial policy instruments, but remains exposed to fragility at lower tiers.

Across contexts, the key issue is not whether firms accept the legitimacy of security objectives, but whether the **burden-sharing arrangement is perceived as fair and sustainable**. Where costs are seen as excessive or arbitrarily imposed, firms tend to comply formally while minimizing deeper integration.

5.4 Legal and Regulatory Friction as an Unintended Constraint

Another recurring theme is the tension between economic security objectives and existing legal frameworks. Competition law, subcontracting rules, data protection regimes, and environmental regulation can all inhibit supply chain restructuring—even when governments explicitly call for diversification or trusted sourcing.

The South Korean “Tier-1 wall” is a particularly clear example, but similar dynamics appear in Australia through overlapping export control regimes and in Finland through the need to carefully balance preparedness with EU internal market rules. These frictions are rarely the result of policy neglect; rather, they reflect the fact that most legal frameworks were designed for a different economic era.

Trusted supply chain governance therefore requires **regulatory coherence across domains**, not just new security instruments layered on top of existing rules. Without such coherence, firms face contradictory obligations that slow adaptation and increase compliance risk.

5.5 Trust, Information, and the Limits of Voluntarism

Trusted supply chains ultimately depend on trust—not as a political slogan, but as an operational condition. Firms must trust that governments will handle sensitive information responsibly, apply rules predictably, and intervene proportionately during crises. Governments must trust that firms will act in good faith, share relevant risk information, and prioritize continuity when markets are stressed.

The Finnish model demonstrates how such trust can be institutionalized through long-standing public-private structures, but it also highlights the difficulty of replicating this approach in environments with lower baseline trust or more adversarial state-business relations. Australia’s experience with information-sharing mechanisms such as TISN shows that even well-designed platforms can suffer from engagement fatigue if firms perceive asymmetrical risk.

South Korea’s more directive model avoids some of these problems through hierarchy and legal mandate, but at the cost of reduced flexibility and heavier administrative load.

The comparative lesson is that **voluntarism alone is insufficient**, but heavy-handed control can undermine innovation and responsiveness. Sustainable trusted supply chains require calibrated governance that combines incentives, obligations, and credible reciprocity.

5.6 From Friction to Dialogue: Implications for Public-private Coordination

Taken together, the findings point to a central conclusion: trusted supply chains cannot be delivered through policy instruments alone. They require **structured, sustained public-private dialogue** focused not on abstract alignment, but on resolving concrete implementation frictions.

Across the three country cases, recurring dialogue priorities emerge:

- clarifying expectations around supply chain visibility and proportionality;
- reducing regulatory overlap and legal contradictions;
- addressing SME capacity constraints and compliance burdens;
- improving access to risk-relevant information without creating liability traps;
- and aligning allied frameworks to reduce duplication in export controls and security requirements.

These are not one-off problems to be solved through legislation or funding alone. They are ongoing governance challenges that evolve alongside technology, geopolitics, and market structure.

5.7 Takeaway: Trusted Supply Chains as a Workable Bargain

The evidence presented in this report suggests that trusted supply chains are best understood as a **workable bargain** between governments and firms. Governments seek resilience, continuity, and security alignment; firms seek predictability, proportionality, and commercial viability. Where this bargain holds, security objectives become internalized within corporate strategy. Where it breaks down, trust erodes and policy effectiveness declines.

The cases of Australia, Finland, and South Korea show that there is no single institutional model for achieving this balance. But they also demonstrate that success depends less on the choice between markets and states, and more on the quality of governance linking them.

This insight provides the foundation for the concluding chapter, which synthesizes the report's findings and outlines pathways for strengthening trusted supply chains through practical, dialogue-driven coordination among the United States and its partners.

Taken together, these findings point to a need for structured, partner-driven coordination platforms capable of translating strategic alignment into operational practice. Without such mechanisms, trusted supply chain policies risk remaining declaratory—strong on intent, but uneven in execution across firms, sectors, and jurisdictions.

Chapter 6: Conclusions and Policy Recommendations

6.1 From Strategic Alignment to Operational Reality

This report has shown that trusted supply chains are not failing because of a lack of political alignment or policy activity. Across Australia, Finland, and South Korea, governments have adopted increasingly sophisticated economic security frameworks, and firms operating in dual-use and defense-adjacent sectors demonstrate a high degree of awareness of geopolitical risk. Strategic intent is present, institutional architectures are evolving, and the language of trust, resilience, and de-risking is now firmly embedded in policy discourse.

The core challenge lies elsewhere: in the translation of strategic intent into firm-level incentives, operational clarity, and workable governance arrangements. Trusted supply chains ultimately depend on whether companies can internalize security objectives without undermining competitiveness, innovation, or commercial viability. Where that balance is poorly managed, resilience remains aspirational and compliance becomes superficial. Where it is governed credibly—through predictable rules, proportional obligations, and tangible participation value—firms adapt their strategies and investment decisions accordingly.

A central conclusion of this report is therefore that trusted supply chains are best understood as a **shared governance challenge**, not a unilateral policy project. Governments shape the strategic environment through regulation, alliance frameworks, export controls, and public investment. Firms, in turn, operationalize trust through sourcing decisions, supply chain design, risk management, and organizational choices. Failure on either side weakens the system as a whole. This interdependence explains why trusted supply chains cannot be delivered through declarations of alignment alone, nor through compliance-heavy approaches that ignore commercial realities.

The empirical evidence from Australia, Finland, and South Korea demonstrates that trusted supply chains do not emerge automatically from political alignment. They are constructed through continuous negotiation between security objectives and commercial realities—across legal frameworks, cost structures, information asymmetries, and organizational capacity. This chapter therefore focuses on how that negotiation can be made more effective.

Across the three country cases, trusted supply chains function best where they are underpinned by a **workable bargain** between the public and private sectors:

- Governments seek resilience, continuity, and alignment with allied security frameworks.
- Firms seek predictability, proportionality, and commercial viability.

Where this bargain holds, security objectives become internalized into corporate strategy rather than treated as externally imposed compliance costs. Where it breaks down, firms rationally minimize exposure, delay investment, or retreat to formalistic compliance without deeper integration.

This insight cuts across institutional models. Finland’s trust-based, institutionalized approach; Australia’s alliance-embedded, incentive-driven system; and South Korea’s law-centered, state-orchestrated model differ markedly in form. Yet all face similar stress points at the implementation layer: visibility gaps beyond Tier-1 suppliers, uneven distribution of compliance costs, regulatory friction across legal domains, and participation fatigue in public-private engagement mechanisms.

The recommendations that follow are designed to address these shared challenges. They focus not on creating new grand strategies, but on improving **how existing strategies are executed**—by clarifying expectations, aligning incentives, and strengthening the governance interfaces between states and firms.

6.2 Policy Recommendations

Recommendation 1: Operationalize “Trusted Partner” Status Across Allied Supply Chains

Problem addressed: Firms increasingly rely on informal signals—alliances, treaties, political alignment—to infer trustworthiness. This creates uncertainty, slows collaboration, and raises compliance costs, particularly for SMEs operating in dual-use sectors.

What needs to change: Trusted partnership must move from political designation to operational status through:

- shared baseline criteria (export control alignment, IP protection, cyber maturity);
- mutual recognition mechanisms (pre-cleared suppliers, reciprocal audits, license-free or fast-track environments in defined domains);
- clear escalation and suspension rules when trust conditions are breached.

Who needs to act: U.S. and allied governments (export control and defense authorities), allied coordination forums, and firms seeking trusted status through demonstrable compliance and governance maturity.

Why it matters: Without operational trust, “trusted supply chains” remain rhetorical. Formalizing trust reduces friction, accelerates collaboration, and makes resilience commercially viable.

Recommendation 2: Improve Tier-2 and Tier-3 Supply Chain Visibility Without Overburdening Firms

Problem addressed: Visibility deteriorates sharply beyond Tier-1 suppliers—precisely where strategic vulnerabilities often concentrate—while firms often lack legal authority or capacity to map deeper tiers.

What needs to change: Governments and industry should support risk-based, proportionate visibility through:

- shared mapping and analytics platforms for critical inputs;
- legal safe harbors enabling deeper-tier inquiries without breaching competition or subcontracting law;
- targeted SME support for mapping and reporting obligations.

Who needs to act: Economic security units, competition authorities, defense procurement agencies, industry associations, and lead firms coordinating supply chain visibility efforts.

Why it matters: System-level resilience cannot be achieved if the most fragile nodes remain opaque. Visibility must improve without turning compliance into a market barrier.

Recommendation 3: Reduce the “Security Premium” Associated with Trusted Supply Chains

Problem addressed: Trusted or allied sourcing often carries higher costs than globally optimized supply chains, discouraging firms from deeper integration unless compensated through value or risk sharing.

What needs to change: Governments should explicitly address the cost differential by:

- using co-investment, demand aggregation, and long-term offtake commitments;
- prioritizing trusted suppliers in public procurement and export pipelines;
- recognizing resilience investments as strategic assets rather than inefficiencies.

Who needs to act: Treasuries, defense and infrastructure buyers, export credit agencies—and firms by making resilience costs visible in strategic planning and investment decisions.

Why it matters: If resilience is treated solely as a private cost, firms will rationally underinvest. Trusted supply chains require shared burden-sharing.

Recommendation 4: Align Export Controls and Compliance Regimes Among Trusted Partners

Problem addressed: Even among close allies, regulatory misalignment—particularly in export controls—creates delays, uncertainty, and duplicated compliance burdens.

What needs to change: Trusted partners should pursue:

- mutual recognition of export control decisions;
- expanded license-free or fast-track regimes in defined technology domains;
- joint guidance and shared compliance assurance frameworks.

Who needs to act: Export control authorities, defense ministries, allied coordination mechanisms—and firms through early engagement and transparent compliance practices.

Why it matters: Misaligned controls undermine the trust they are meant to protect and slow collaboration in fast-moving dual-use technologies.

Recommendation 5: Treat Public-private Cooperation as a Governance System, Not a Consultation Exercise

Problem addressed: Firms are increasingly treated as security actors, yet engagement mechanisms often remain ad hoc, consultative, or crisis-driven.

What needs to change: Public-private cooperation should be institutionalized through:

- standing dialogue formats linked to concrete policy levers;
- clear expectations on information sharing, protection, and liability;
- predictable value propositions for firms (market access, capability uplift, regulatory clarity).

Who needs to act: National governments, sectoral regulators, defense and economic security authorities—and corporate leadership committing resources and senior accountability to engagement.

Why it matters: Trusted supply chains depend on sustained cooperation. Without a stable governance bargain, participation fatigue and compliance resistance will grow.

6.3 Implementation Map: Translating Recommendations into Action

Table 4 consolidates the recommendations into a **stakeholder-oriented implementation map**, clarifying roles and responsibilities across the public-private divide.

Table 4. Strategic Recommendations – Implementation Map

Stakeholder	Recommended Actions
U.S. Government	• ITAR reform: Accelerate creation of license-free or fast-track environments for vetted allies to reduce regulatory drag on joint development. • SOSA expansion: Provide clearer trusted-partner certifications and joint visibility tools to share supply-chain “red flags” without compromising commercial secrecy.
Allied Governments	• Intelligence-led risk sharing: Shift from compliance-heavy approaches toward declassified, actionable guidance on high-risk sectors and entities. • Regulatory streamlining and harmonization: Accelerate permitting, export approvals, and defense-related facility authorizations to reduce administrative friction in trusted supply chains.
Corporate Leaders	• Geopolitical muscle: Establish senior responsibility (e.g. Chief Geopolitical Officer or equivalent) to integrate security logic into board-level governance and fiduciary duty. • Modular resilience: Adopt modular product and system designs enabling rapid substitution of compromised inputs. • R&D internalization: Strategically localize or internalize core technologies to reduce exposure to chokepoint jurisdictions.

6.4 Final Takeaway

Trusted supply chains are not built through declarations of alignment alone. They emerge where states and firms strike a credible governance bargain—one that aligns security objectives with commercial incentives, clarifies expectations, and shares the costs of resilience. The experiences of Australia, Finland, and South Korea show that this bargain is achievable, but only when policy moves decisively from intent to execution.

Without structured, partner-driven coordination platforms capable of translating strategic alignment into operational practice, trusted supply chain strategies risk remaining declaratory: strong on intent, but uneven in execution across firms, sectors, and jurisdictions.

List of Acronyms

AI	Artificial Intelligence
ASCA	Advanced Strategic Capabilities Accelerator
CIPE	Center for International Private Enterprise
CIRMP	Critical Infrastructure Risk Management Program
DAPA	Defence Acquisition Program Administration
DCA	Defense Cooperation Agreement
DDE	Digital Defense Ecosystem
DIDS	Defense Industry Development Strategy
DTCT	Defense Trade Cooperation Treaty
EU	European Union
EWS	Early Warning System
FDI	Foreign Direct Investment
GSP	Global Supply Chain
GWEO	Guided Weapons and Explosive Ordnance
IP	Internet Protocol
ISR	Intelligence, Surveillance, and Reconnaissance
ITAR	International Traffic in Arms Regulations
JSCFADT	Joint Standing Committee on Foreign Affairs, Defense and Trade
NATO	North Atlantic Treaty Organization
NESA	National Emergency Supply Agency
NESO	National Energy System Organization
NRF	National Reconstruction Fund
OSCR	Office of Supply Chain Resilience
R&D	Research and Development
SDIPs	Sovereign Defense Industrial Priorities
SME	Small and Medium-sized Enterprise
SOCI	Security of Critical Infrastructure Act
SOSA	Security of Supply Arrangement
THAAD	Terminal High Altitude Area Defense
TISN	Trusted Information Sharing Network



CENTER FOR INTERNATIONAL PRIVATE ENTERPRISE

1401 Eye St. NW, Suite 600 | Washington, DC 20005

P: 202.721.9200 | F: 202.721.9250