THE FUTURE OF SECURITY

BRIEFING NOTE FROM THE CENTRE FOR ECONOMIC SECURITY (CES) AND ECCRG/KING'S COLLEGE FUTURE OF SECURITY CONFERENCE

Centre for Economic Security

2025

BRIEFING NOTE FROM THE CENTRE FOR ECONOMIC SECURITY (CES) AND ECCRG/KING'S COLLEGE FUTURE OF SECURITY CONFERENCE

23rd-24th July 2025
King's College, London

Editors:
Dr. Rebecca Harding, CEO, Centre of Economic Security
rebeccaharding@ces-global.net

Lt Gen (Retd) Richard Wardlaw CB, OBE, Chair, Centre for Economic Security
ces-global-net

This briefing summarises the outcomes of the **Future of Security Conference**, hosted at **King's College London** in partnership with the **Economic Conflict and Competition Research Group (ECCRG)** and The **Centre for Economic Security (CES)**. The event was convened in response to growing concerns around the UK and NATO about economic security and the usefulness of current frameworks, including NATO's Articles 2 and 3, for addressing some of these concerns. The event brought together groups that do not often meet from government, financial services (especially trade finance), the defence industrial base and fintechs. The goal was to create a shared vision across these stakeholders of what an economic security manifesto would look like.

The core recommendation of the event was the establishment of a central coordinating function, a National Economic Security Centre, to identify and monitor economic threats, and to develop strategies for ensuring that the UK's economy is resilient and can recover from economic attacks but also use economic and financial power levers offensively. Many of the detailed recommendations would be coordinated by such a function

This summary sets out the strategic context as articulated by the participants, one that sees the UK and its allies engaged in an undeclared economic, indeed multi-domain, conflict. There was a strong sentiment amongst participants at the event that economic orthodoxy will not deliver the required economic security necessary to underpin prosperity and growth. The proposals in the document are from the senior delegates who attended the two days. The Centre for Economic Security (CES) is committed to convening such conversations and working to integrate the shared economic security interests of finance, business and government by helping to implement the vital manifesto that delegates gave us at the Future of Security event.

- **Day One (23 July 2025)** convened s**enior figures from defence,finance, industry, government, and academia,** with a strong focus on the role of SMEs, banks, and institutional investors. Workshops and discussions explored how economic security could be strengthened with a deeper understanding of trade and supply chain finance, working capital and their role in fostering supply chain

resilience and innovation. Special attention was given to the barriers faced by SMEs, the reluctance of banks to support defence, and the need for new instruments to mobilise private capital.

- **Day Two (24 July 2025)** brought together a **strategic and policy-level audience,** including senior MoD officials, financiers, academics, and business leaders. The sessions tested policy options against the wider backdrop of the UK's **Trade Strategy, Strategic Defence Review (SDR)** 2025, and the **Modern Industrial Strategy**. Discussions shifted from identifying problems to formulating prescriptions: embedding whole-of-society mobilisation, reframing ESG to include security, and considering institutional reforms such as a "Ministry of Economic Warfare."
- Across both days, the message was consistent: the UK must **acknowledge that it is already engaged in an economic conflict** and move from analysis to execution. Delayed action would guarantee a reactive, fragmented response. The purpose of this briefing is to capture the conference's conclusions and outline a policy framework that ministers can use to integrate economic security with trade, defence, and industrial policy.

Editors:
Dr. Rebecca Harding, CEO, The Centre of Economic Security
rebeccaharding@ces-global.net

Lt Gen (Retd) Richard Wardlaw CB, OBE, Chair, Centre for Economic Security
ces-global-net

Strategic Context – The Age of Economic Warfare

The UK is already engaged in an **economic conflict**. Adversaries and sometimes even allies are using trade restrictions, cyber interference, financial coercion, and manipulation of critical infrastructure as strategic weapons. At the conference, participants pointed to a single day in April that saw: EU officials advised to use burner phones in the US; the UK re-nationalising British Steel on security grounds; China interfering with undersea cables; and Germany altering missile support to Ukraine after a Russian strike. These were not random headlines but **battle reports in an undeclared war**.

The **post–Cold War assumption of stability and globalisation is over**. The SDR 2025 makes clear that the rules-based order has eroded, state-on-state confrontation has returned, and "resilience" alone is not sufficient. As one senior participant observed: *"We're trying to fight 21st-century wars with 20th-century procurement and 19th-century bureaucracy."*

The economic dimension is now central to deterrence. Former military leaders stressed that **"you can't deter if you can't endure"** — and endurance comes as much from factories, farms, fibre-optic cables, and finance as from frigates and fast jets. The UK Trade Strategy calls for supply chain diversification and reduced dependency on fragile global systems. The Modern Industrial Strategy highlights the need to leverage innovation, technology, and private capital for national resilience.

Finance and Investment Reform – Unlocking the "Longest Purse"

Banks remain reluctant to fund defence-related projects. Compliance burdens (sanctions, export controls, KYCC), reputational risk, ESG pressures, and lack of political cover make finance houses default to "no." As one banker admitted candidly: *"We will all finance barracks, but we also need to finance things that go bang."*

This reluctance creates a **strategic vulnerability**: adversaries understand that financial hesitancy can be weaponised to constrain the UK's ability to sustain conflict. Financial institutions emphasised that they cannot act alone; government must provide both a **"fig leaf" of legitimacy** and the **policy cover** to align national security objectives with fiduciary duty.

Policy actions to consider include:

- **Defence & Infrastructure Finance Charter**: A co-developed framework with banks, setting risk-sharing principles, ESG alignment criteria, and clear guidance on permissible activities. As participants argued: *"If your supply chain can be weaponised against you, it's a governance failure — and an existential one."*
- **Government-backed guarantee schemes**: Expansion of credit guarantees, first-loss capital, and blended finance instruments to de-risk lending.
- **New financial products**: Long-term credit aligned to defence innovation cycles, insurance mechanisms for regulatory risk, and pooled liquidity facilities for SMEs.
- **Reframing ESG**: Shift from "Environment, Social, Governance" to include **Security.** This means including Security as a means of providing societal returns on investment in the same way that food, energy and health security do.

These steps align with the Industrial Strategy's focus on mobilising private investment into strategic sectors, and the Trade Strategy's priority of building resilient, sovereign capabilities.

SMEs and Innovation Ecosystem – Strategic Assets, Systemic Barriers

SMEs provide much of the **niche innovation** and supply-chain resilience that modern warfare demands. Yet over 90% operate under primes, face cash-flow crises, and are boxed out of procurement because of compliance hurdles. Many SMEs reported that *"banks don't fund us because we don't fit into boxes."*

At the Hackathon, SMEs described MoD payment protocols as **crippling**: they must complete programmes before payment, leaving smaller firms unable to cover wages, tooling, or overheads. Banks, meanwhile, continue to penalise them for pandemic-era downturns, ignoring current growth or strategic contracts.

Suggested policy actions:

- **Single Due Diligence Digital Badge**: A "passport" certification system, earned once and trusted by banks and government, to cut compliance duplication.
- **Fast-track SME pathways**: Regulatory and licensing shortcuts alongside specific credit risk and insurance assessments for vetted SMEs
- **Innovation funds**: Building on the announcements in the Strategic Defence Review to work with providers of private credit supply debt-based working capital to SMEs
- **SME Defence Label**: Tiered certification, internationally recognised, giving SMEs tangible benefits (better credit terms, faster vetting, trusted access to contracts).

Participants were of the view that without these reforms, the UK risks losing its innovation edge, as adversaries more seamlessly integrate state and commercial capacity. The security consequences of this recommendation would need to be considered in order to ensure that defence sub-contractors cannot be identified outside of the financial framework as being part of a defence supply chain. One idea would be to use the mechanisms developed in digital trade finance where increasingly transactions are tokenised.

Supply Chain and Industrial Resilience – Redundancy by Design

The UK remains **exposed to fragile supply chains**: during COVID, over 80% of military clothing was sourced from a single province in China. Reliance on single sources, just-in-time models, and foreign ownership of strategic assets is an open invitation to adversaries.

Participants stressed the need for **redundancy by design**. This requires mapping supply chains to the raw material level, establishing multiple sourcing options, and deliberately dispersing production. Clusters may deliver efficiency, but they also create concentrations that adversaries can target.

Suggested policy actions:

- **Critical supply chain mapping**: Develop a national database to trace key inputs and vulnerabilities.
- **Surge capacity funding**: Government co-investment in "slack" production capacity, even if underutilised in peacetime.
- **Geographic dispersion**: Avoid co-location of critical infrastructure by funding parallel facilities in diverse regions, or in foreign locations.
- **Stockpiles and redundancy**: Treat surplus not as waste but as strategic insurance against shocks.

This approach delivers on the SDR's call for endurance, the Trade Strategy's commitment to resilient sourcing, and the Industrial Strategy's priority of securing sovereign supply chains.

Editors:
Dr. Rebecca Harding, CEO, Centre of Economic Security
rebeccaharding@ces-global.net

Lt Gen (Retd) Richard Wardlaw CB, OBE, Chair, Centre for Economic Security
ces-global-net

Data and Intelligence Infrastructure – Closing the Blind Spots

Across all sessions, participants highlighted the **data deficit**. Banks, industry, and government all lack timely, shared, actionable intelligence on supply chain risks, financing patterns, and adversary activities. This leaves dangerous blind spots and drives institutions towards risk aversion.

Solutions proposed included:

- **Financial Common Operational Picture (FIN COP)**: A secure platform enabling real-time sharing of financial, supply chain, and threat data across government, banks, and industry. It was acknowledged that this structure would need careful thought and perhaps coordinated through a centralised National Economic Security Centre.
- **Single Due Diligence Badge**: A digital credential system for SMEs, streamlining compliance and giving banks confidence.
- **Clean Public–Private Data Networks**: Secure, "trusted" channels for sharing cyber threat intelligence, foreign influence risks, and supply chain vulnerabilities.

The absence of such systems leaves the UK behind adversaries who have already integrated financial intelligence with national strategy. Building this capability would reinforce the SDR's commitment to whole-of-society resilience and the Industrial Strategy's focus on digital competitiveness.

Editors:
Dr. Rebecca Harding, CEO, Centre of Economic Security
rebeccaharding@ces-global.net

Lt Gen (Retd) Richard Wardlaw CB, OBE, Chair, Centre for Economic Security
ces-global-net

Institutional Reform – From Peacetime to Preparedness Mode

Governance remains fragmented and slow. Multiple departments and agencies own different aspects of economic security, but no one body is responsible for coordination. As participants remarked: *"When everyone owns it, no one owns it."*

Several proposals emerged for a **central coordinating body** — a "Ministry of Economic Warfare" or Cabinet Office-led unit — empowered to unify strategy, intelligence, and crisis response. Such a central coordinating body would be a National Economic Security Centre and would map the structures of the National Cyber Security Centre to provide similar Economic Security focus. Its functions would include coordinating with allies, liaising with finance and industry, and running a standing operations room for economic security.

Institutional culture must also shift. Resilience cannot mean bureaucracy and delay; it must mean **adaptability and speed**. War is a "measure–countermeasure" cycle — sanctions will be evaded, supply chains attacked, cyber defences breached. Institutions must be able to pivot continuously.

This requires:

- Delegated decision-making authority.
- Built-in redundancy and rapid adaptation cycles.
- Permanent cross-sector representation (finance, industry, academia, government).
- A narrative shift that frames defence and economic security as a **public good** — essential for prosperity, democracy, and resilience.

Public Narrative and Legitimacy – Mobilising Support

A recurring theme was the need to **mobilise society**. Defence cannot be the preserve of the MoD. As Chris Donnelly argued: *"War is not just about missiles; it is fought by whole countries. Every government department and every citizen has a role."*

Yet political legitimacy is fragile. Citizens naturally prefer welfare to warfare, "pip and potholes" to missiles. Governments must make the case that defence is not a drain on prosperity but a **precondition for it**. Public-facing messaging should emphasise that investing in security is about protecting communities, jobs, and daily life.

Proposed actions include a **national communications campaign**, **Citizen preparedness initiatives** and a **refocus on security as part of the ESG frameworks**. Understanding threats and mobilising society and the economy accordingly would be a core function of the National Economic Security Centre.

Editors:
Dr. Rebecca Harding, CEO, Centre of Economic Security
rebeccaharding@ces-global.net

Lt Gen (Retd) Richard Wardlaw CB, OBE, Chair, Centre for Economic Security
ces-global-net

Conclusion – From Analysis to Execution

The Future of Security conference and subsequent workshops produced a consistent message: **delay guarantees failure**. Without decisive action, the UK risks being outpaced by adversaries who already integrate economic and military planning.

The means of coordinating this approach will be through the establishment of a National Economic Security Centre which uses the established framework of the National Cyber Security Centre to identify threats and coordinated responses and preparedness for those threats.

The SDR 2025, UK Trade Strategy, and Modern Defence Industrial Strategy and the National Security Strategy provide the political mandate.

This briefing sets out the operational direction:

- **Reframe defence as a public good**.
- **Mobilise private finance with political cover**.
- **Support SMEs as strategic assets**.
- **Build supply chain redundancy and resilience**.
- **Create shared intelligence infrastructure**.
- **Reform institutions for wartime adaptability**.

These steps are not discretionary. They are necessary to protect the UK's sovereignty, prosperity, and democratic resilience in an era where economics and security are inseparable.

As one senior defence leader remarked at the end of the event, 'We must stop admiring the problem. Now is the time for action.

Editors:
Dr. Rebecca Harding, CEO, Centre of Economic Security
rebeccaharding@ces-global.net

Lt Gen (Retd) Richard Wardlaw CB, OBE, Chair, Centre for Economic Security
ces-global-net

Appendix – policy recommendations

The policy recommendations that emerged were wide-ranging but coherent:

- Reframe defence as a public good and embed it in economic narratives.
- Establish a Defence and Infrastructure Finance Charter with clear rules for government, banks, and SMEs.
- Create compliance passports and working capital guarantees for SMEs.
- Develop a FIN COP and a Single Due Diligence Digital Badge.
- Establish a Ministry (or Shadow Ministry) of Economic Warfare.
- Map and diversify supply chains, fund redundancy by design.
- Foster an innovation culture tolerant of risk and failure.
- Design offensive economic tools alongside defensive measures.
- Mobilise society as a whole into a preparedness economy.

The significance of the conference lies not only in its specific proposals but in the act of convening diverse constituencies to develop a common language and shared agenda. Banks, SMEs, tech firms, and government rarely sit together in this way. The event demonstrated both the scale of the challenge and the possibility of building consensus. The urgency was underlined repeatedly: delay will guarantee a reactive, fragmented response when crises escalate. *"If you can't make it, move it, or fix it when it breaks, you don't own it — your adversary does."*