THE FUTURE OF SECURITY

CENTRE FOR ECONOMIC SECURITY AND ECCRG KING'S COLLEGE, LONDON

23RD AND 24TH JULY, 2025 GUIDEHOUSE, 1, ANGEL COURT, LONDON AND KING'S COLLEGE LONDON

EVENT SUMMARY

Centre for Economic Security

2025

CONTRIBUTORS

Dr. Heiko Bochert
Dr. Jack Harding
Dr. Rebecca Harding
Mr. Bryce G. Hoffman
Professor Greg Kennedy
Dr. Ksenia Kirkham
Dr. Maria Papageorgiu

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Future of Security Conference, held on 23–24 July 2025 at King's College London under the Chatham House Rule, brought together senior leaders from government, defence, security, banking, finance, technology, academia, and the SME sector to grapple with one of the most pressing questions of our time: how to understand, prepare for, and respond to the realities of economic warfare and economic security in the 21st century.

The event was structured over two complementary days. Day 1 adopted an innovative hackathon-style format, convening four specialist groups — defence and security SMEs, banks and finance providers, technology and data companies, and government representatives. These groups were tasked with addressing two urgent questions: first, how to make banks comfortable with funding defence and security SMEs; and second, what would be required to set up a Shadow Ministry of Economic Warfare to build preparedness. Day 2 was a formal, high-level conference attended by senior officials, industry leaders, financiers, and academics. The aim on this second day was to define the concepts of economic warfare and economic security, and to generate actionable policy recommendations to create a preparedness economy fit for the current threat environment.

Taken together, the two days provided both bottom-up innovation and top-down policy framing. Day 1 surfaced the pain points, structural barriers, and practical proposals from those directly involved in defence finance, innovation, and government. Day 2 elevated these findings into a strategic conversation about how to reshape the UK's institutions, finance systems, and industrial base to deal with the reality that the country is already in an economic war. The continuity between the two days was deliberate: the hackathon was designed to expose systemic obstacles, and the formal conference used those outputs as the scaffolding for more detailed debate.

The context for the conference is stark. For the past eight decades, much of the Western world operated within what was assumed to be a secure, stable, and rules-based international order. That order is now fracturing. The assumptions of globalisation, economic interdependence, and security through trade have collapsed. Instead, adversaries are weaponising interdependence itself. Energy, food, finance, technology, data, and critical materials have all been turned into levers of coercion and disruption. ***"We are now at war, even if people are reluctant to admit it,"*** as one participant put it. Another added, "***We are trying to fight 21st-century wars with 20th-century procurement and 19th-century bureaucracy."***

In this environment, economic statecraft is not an adjunct to military force; it is a primary domain of conflict. Sanctions, supply chain interference, cyber disruption, and financial manipulation are deployed daily as weapons. Wars are decided as much by resilience, redundancy, and the ability to mobilise finance and production at speed as by military hardware. Yet Western institutions — governments, banks, regulators, procurement systems — remain largely optimised for peacetime efficiency rather than wartime adaptability. The Future of Security Conference was a direct attempt to confront this paradox.

Day 1 revealed a series of systemic misalignments. Banks emphasised reputational risk, onerous compliance regimes, and the absence of clear political signals as reasons for their reluctance to fund defence SMEs. ***"All of us will finance barracks,"*** one banker admitted, ***"but we also need to finance things that go bang."*** SMEs highlighted the cash-flow crises generated by Ministry of Defence payment protocols, as well as their structural dependence on prime contractors. Tech companies expressed frustration at data silos and the lack of transparent, accessible information from both government and finance. Government participants, for their part, acknowledged inertia and institutional fragmentation.

Despite these frustrations, solutions began to emerge. A Single Due Diligence Digital Badge was proposed to streamline compliance and give banks confidence. A Financial Common Operational Picture (FIN COP) was recommended to integrate intelligence on supply chains, finance flows, and threat exposure. Reforms to MoD payment structures and the creation of working capital guarantees for SMEs were discussed. The need for a Shadow Ministry of Economic Warfare was discussed to cut across silos and coordinate at speed. As one participant summarised, ***"When everyone owns it, no one owns it."***

Day 2 built directly on these outputs. Senior participants acknowledged that economic resilience is as vital as military strength. ***"You can't deter if you can't endure,"*** one noted. The private sector was recognised as a frontline actor in national security, though cultural and fiduciary barriers persist. Speakers argued for reframing ESG to include Security, embedding defence within the broader narrative of economic growth, technological competitiveness, and societal resilience. Debates focused on five areas: finance and institutional reform; innovation and risk culture; SME ecosystem strengthening; supply chain resilience; and offensive economic statecraft.

Proposals included establishing a Defence and Infrastructure Finance Charter co-developed with industry, creating loss absorption funds to de-risk strategic projects, and developing compliance passports for SMEs. The Ministry of Economic Warfare concept resurfaced, now framed as essential to unify strategy and act as a single point of contact for industry and allies. The balance between centralisation and decentralisation was repeatedly emphasised: scale is necessary for major platforms, but dispersed innovation and redundancy are vital for resilience. Offensive economic tools were also debated, with calls to design digital blockades, financial disinformation campaigns, and bloc-scale wartime protocols. ***"Money is the fastest weapon we have — but right now, it's locked in the armoury,"*** observed one voice.

Across both days, several cross-cutting themes became clear. First, the government must send clear, bipartisan signals to provide banks with political cover and to frame defence as a public good. Second, SMEs are strategic assets but remain systemically fragile; they require tailored support. Third, shared data and intelligence are essential to overcoming information asymmetries. Fourth, resilience depends on a hybrid model that combines efficiency with redundancy and adaptability. Fifth, economic warfare requires both defensive and offensive tools; deterrence depends on the credible capacity to impose costs as well as absorb them.

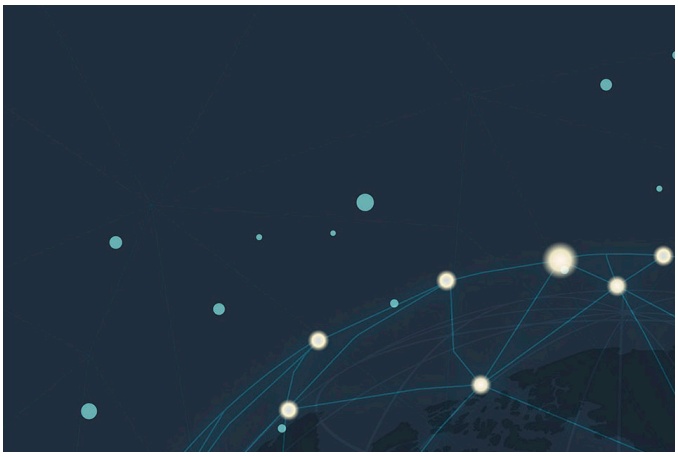
The policy recommendations that emerged were wide-ranging but coherent:

- 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 National Economic Security Centre, aligned closely with the activities and structures of the National Cyber Security Centre
- 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."***

In sum, the Future of Security Conference represented a turning point. It acknowledged that the UK is already engaged in economic warfare, howsoever unpalatable that word is in defence and security circles. The use of the word war was not uncontested amongst delegates, but the fact that every method of fighting economic war is in play now or has been in play over the past few years, justifies its use in this document and accurately reflects the tone of the two days.

It surfaced systemic barriers and offered practical solutions; it built continuity from grassroots problem-solving to strategic debate; and it produced a coherent set of policy recommendations. The task ahead is to move from analysis to execution, ensuring that institutions, finance, and industry are fit for the demands of the new era.



CENTRE FOR ECONOMIC SECURITIES

INTRODUCTION: CONTEXT & CHALLENGE OF THE ERA

The Future of Security Conference took place against the backdrop of a profound rupture in the international system. For most of the post-war period, Western democracies operated within a framework of stability and predictability. Economic interdependence, multilateral institutions, and shared rules provided both prosperity and security. Many assumed that this system had become permanent. Yet by mid-2025, that assumption has collapsed.

Speakers at the conference framed this change with clarity and urgency. One described it as a moment of collective denial: ***"For eighty years we have lived inside a rules-based system and assumed it was permanent. That system is gone, and our institutions are no longer fit for purpose."*** Others warned that Western societies have been slow to recognise the implications. ***"It is easier to dismiss this as exaggeration than to confront the upheaval required,"*** noted one contributor. The reluctance to face reality, they argued, leaves democracies vulnerable to surprise and exploitation.

The global environment is now one of volatility, uncertainty, and systemic competition. Adversaries employ every tool of power short of open conventional warfare — and sometimes beyond it. Information, cyber, finance, trade, energy, and critical infrastructure have all become weaponised. This is more than "strategic competition": it is a form of economic war being fought daily in financial markets, supply chains, and data networks. ***"Today's warfare is not just about bombs and missiles,"*** as one participant emphasised. ***"In today's total war, everything is a weapon."***

This recognition forces a conceptual shift. In the past, economics was seen as the background condition for war: a factor of production to support military campaigns. Today, economics is itself a primary battlespace. Disinformation campaigns disrupt societies; sanctions and countersanctions seek to cripple adversaries; cyber-attacks paralyse infrastructure; and financial markets are manipulated as strategic instruments. Julian Corbett's early twentieth-century insight that ***"finance is scarcely less important than force"*** has acquired renewed relevance.

For the UK, this context creates acute vulnerabilities. The country is heavily dependent on global supply chains for critical minerals, technologies, and food. Domestic surge capacity in defence production is limited after decades of offshoring and just-in-time efficiency. As one participant warned, "***If you can't make it, move it, or fix it when it breaks, you don't own it — your adversary does."*** Many national institutions, from procurement systems to financial regulators, remain optimised for peacetime assumptions of stability rather than the turbulence of conflict. Universities depend on foreign student funding even as their research outputs flow abroad. Food security is partial at best: the UK produces little more than half of its needs. Infrastructure ownership is scattered across foreign investors, some potentially hostile.

This fragility is compounded by cultural expectations shaped by decades of stability. Citizens have become accustomed to predictability and control. Yet wartime conditions mean uncertainty, disruption, and constant adaptation. ***"We must come to terms with unpredictability and danger,"*** one participant insisted. ***"Peacetime efficiency must give way to wartime resilience."*** That resilience requires not only new tools but also a new mindset. Instead of control, command and delegation must be emphasised. Grassroots initiative and rapid decision-making must be empowered. Risk-taking must be rewarded, even when it leads to failure. ***"We must work by trial and error, not as today by error and trial,"*** one speaker observed pointedly.

At an institutional level, this implies a permanent state of adaptability. In wartime, every move generates a countermove. In the Second World War, tanks produced anti-tank weapons; countermeasures evolved quickly. The same cycle applies today not just to weapons systems but to every economic lever: sanctions, cyber tools, trade restrictions, finance mechanisms. Adversaries adapt, evade, and retaliate. Periodic reviews and occasional strategies are inadequate. Institutions must be capable of continuous learning and rapid adjustment. ***"What we do not need is another strategy document gathering dust,"*** one voice warned. ***"We need institutions that can adapt faster than our enemies."***

The shift from stability to turbulence also forces a reconsideration of redundancy. Efficiency and clustering have been

the watchwords of economic policy for decades. Yet in wartime, efficiency creates vulnerability. Clusters of production invite targeting. Just-in-time supply chains collapse under stress. True resilience requires slack, redundancy, and duplication by design. This is costly and counter-intuitive from a peacetime perspective but essential for survival in protracted conflict. As one participant summarised, ***"Resilience is expensive, but fragility is fatal."***

The nature of adversaries also demands rethinking. States hostile to the UK are not merely competitors but active aggressors employing hybrid and economic warfare as a daily practice. Their aims are not marginal advantage but systemic disruption: eroding cohesion, undermining confidence, and weakening capacity. The challenge is not just to respond tactically but to reconfigure national institutions for a protracted era of conflict.

This in turn raises profound questions about governance. War is not fought by armies alone. It is fought by entire societies. Every government department, every industry, every part of civil society has a role. Yet Western governments have become fragmented, siloed, and in some cases impotent in the face of accelerating change. The question posed repeatedly at the conference was simple: how can these institutions be reshaped for wartime conditions? ***"If we wait for someone else to do it, we will wait too long,"*** one participant challenged.

The answer lies in coordination across society. Government, finance, industry, and academia must be mobilised as a single ecosystem. Citizens must be informed honestly of the stakes and enlisted in support. Alliances must be strengthened, recognising that allies' interests are not always identical but can be aligned through transparency and shared priorities. Above all, leadership is required to break through inertia and drive reform. ***"Leadership now means rapid decision-making with incomplete information,"*** said one speaker. ***"It means action rather than words."***

The challenge is immense. It requires new institutional frameworks, new financial instruments, new industrial models, and a cultural shift in risk and resilience. But the stakes are unavoidable. Without such transformation, Western societies will face crises unprepared and reactively. The conference's purpose was to outline not only the nature of the challenge but the pathways to adaptation.

In sum, the context is one of systemic fragility in an era of economic war. The challenge is to build resilience, adaptability, and offensive as well as defensive capabilities. The era of assuming peace is over. The task now is to mobilise for protracted, hybrid, economic conflict.

DAY 1

HACKATHON & SPECIALIST WORKING GROUPS

The first day of the Future of Security Conference deliberately broke with convention. Rather than opening with set-piece speeches, panels, and pre-cooked policy papers, the organisers convened a hackathon-style working session. The aim was to put four key constituencies — defence and security SMEs, banks and finance providers, technology and data companies, and government representatives — into direct dialogue with one another. This was a recognition that the traditional silos between these groups are themselves part of the problem.

The participants were asked to focus on two simple but urgent questions:

1. How do we make banks comfortable with funding defence and security SMEs?

2. What are the key requirements to establish a Shadow Ministry of Economic Warfare to create preparedness?

The Shadow Ministry of Economic Warfare idea was posed simply to create a stylised view of the need for central coordination. This has morphed into the core recommendation of the two days that there is a need for a coordinating function - a National (or indeed Nato or EU level) Economic Security Centre to identify, manage and prepare for economic threats. Again, the term Shadow Ministry of Economic Warfare is used to reflect what was discussed only.

By stripping the conversation down to these two challenges, Day 1 created a crucible in which participants could air frustrations, compare perspectives, and sketch practical solutions. The outputs were not polished policy documents but raw, candid, and often provocative insights. They became the scaffolding on which Day 2's more formal debates were built.

The Atmosphere: Candour and Frustration

The hackathon atmosphere encouraged honesty. There was no press, no public audience, and no attribution. This freed participants to speak bluntly.

Bankers acknowledged their reluctance to finance defence. ***"All of us will finance barracks,"*** one admitted ruefully, ***"but we also need to finance things that go bang."*** The reasons ranged from compliance burdens to reputational risk, from shareholder sensitivities to geopolitical exposure. ***"You cannot trust the export licensing regime,"*** another banker argued. ***"The weapons last longer than the politics do."***

SMEs voiced equally raw frustrations. Many described the near-impossibility of managing cash flow under Ministry of Defence payment protocols. ***"Government contracts don't pay until the end,"*** one explained, ***"but we need cash up front for tooling, wages, and overheads. By the time the money comes, we're already in debt."*** Others complained of banks penalising them for past downturns. "***They look at our books from five years ago and say, 'You took a hit during COVID, so you're high risk.' We're stuck in the mud."***

Technology companies highlighted opacity and bureaucracy. "***The problem isn't what we don't know,"*** said one technologist. ***"It's what we do know and can't access because the banks won't share data."*** Another compared dealing with large financial institutions to navigating government itself: ***"It's like dealing with the MoD — too many layers, no one empowered to decide."***

Government representatives did not deny these critiques. Several admitted that institutional inertia, risk aversion, and fragmented responsibilities have left gaps. ***"We have a habit of making everything more complicated than it needs to be,"*** one conceded.

The tone was sometimes exasperated but also constructive. The absence of attribution and hierarchy allowed grievances to surface, but also freed participants to explore creative solutions.

Working Group One: Technology & Data

The technology group zeroed in on the barriers created by data silos. Banks, they argued, hold enormous quantities of information on creditworthiness, supply chains, and transactions. Yet internal politics and compliance concerns mean this data is not shared even when it could de-risk lending.

Government was accused of compounding the problem. Agencies, participants argued, are often risk-averse and impose extra layers of red tape. One technologist was blunt: ***"I avoid government whenever I can — they make our work harder, not easier."***

The group proposed two major innovations. The first was the creation of a Financial Common Operational Picture (FIN COP) — a secure platform integrating data from

banks, government, and industry to provide real-time visibility on financial flows, supply chains, and risks. This would function much like a military operational picture, but for the economic domain. The second was the Single Due Diligence Digital Badge: a credential that SMEs could apply for once, demonstrating that they had passed compliance and security checks. Banks could then rely on the badge rather than running duplicative, costly processes each time.

Both ideas reappeared repeatedly on Day 2, demonstrating how Day 1 outputs fed directly into later policy discussions.

Working Group Two: Banks & Finance

The bankers in the room did not disguise their caution. Their reluctance to finance defence companies — especially SMEs — was rooted in several factors:

- Compliance burdens: export controls, anti-money-laundering regimes, and international regulations made lending to defence complex and risky.
- Reputational risk: shareholders, activists, and even other governments often challenged defence finance. ***"We operate internationally,"*** one banker said, ***"and we're answerable to regulators in multiple jurisdictions, not all of whom are comfortable with arms finance."***
- Perceived risk/return imbalance: SMEs often lacked the scale or growth potential of other sectors, making them less attractive investments. ***"Success needs to be measured in more than just pounds,"*** one SME later retorted.

Yet even the bankers acknowledged that their position was unsustainable. Defence, they admitted, is a strategic necessity. One banker suggested that ESG frameworks could be reinterpreted to include Security as the "S": "If ESG becomes ESG+Security, we have a fig leaf we can use with shareholders."

The bankers pressed government to send clearer signals. If government demanded that banks finance rearmament, they argued, it would provide cover. ***"We need the fig leaf from government,"*** as one put it.

The group also acknowledged the need for collective solutions. A banking consortium dedicated to defence lending, backed by public guarantees, was floated. This would spread risk and reduce individual exposure.

Working Group Three: SMEs

The SME group was perhaps the most vocal. Their challenges were stark:

- Cash flow: MoD payment protocols delay revenues until project completion. SMEs must carry costs for months or years without reimbursement.
- Access to credit: banks penalise them for past downturns, especially the COVID period, or refuse to finance defence at all.
- Restrictions: even when financing is provided, banks impose restrictive covenants. ***"Stop telling us what we can't do,"*** one SME complained.
- Return on investment: defence manufacturing offers steady but modest returns compared to sectors like AI. Banks chase high growth, leaving defence SMEs overlooked.

Despite these obstacles, SMEs emphasised their strategic value. They are often the source of innovation, agility, and niche

capabilities. But without financial support, many struggle to survive. One SME was blunt: ***"It's nearly impossible for us to fund the work we do get. We're expected to deliver national security with no oxygen."***

The SMEs supported ideas such as compliance passports, government guarantees, and reforms to MoD payment systems. They also urged greater integration with prime contractors, but on fairer terms.

Working Group Four: Government

Government representatives acknowledged the dilemmas but emphasised constraints. Budget cycles, accountability requirements, and international obligations all limited flexibility. Yet there was recognition that new institutional frameworks might be needed. ***"If we want banks, SMEs, and tech firms to work together, someone has to coordinate,"*** one official said. ***"Right now, that someone doesn't exist."***

This led directly into the second major question of the day: what would it take to establish a Shadow Ministry of Economic Warfare?

The Shadow Ministry of Economic Warfare

The idea of a Shadow Ministry emerged as both provocative and practical. Its purpose would be to coordinate economic statecraft across government and between government and the private sector.

Participants envisioned it as:

- A central hub: integrating intelligence, finance, trade, industry, and technology policy into a coherent strategy.
- A convener: bringing banks, SMEs, primes, and tech firms into structured dialogue under government sponsorship.
- A coordinator with allies: liaising with NATO, the EU, and other partners to harmonise economic warfare measures.
- An incubator: testing experimental approaches in a safe, closed environment before wider rollout.

The key point was speed. Existing institutions were seen as too slow, too fragmented, and too risk-averse. "***When everyone owns it, no one owns it,"*** one participant repeated. A dedicated body would create clarity and accountability.

The concept did not go unchallenged. Some worried about duplication with existing ministries. Others asked whether a "shadow" body could have real authority. But the momentum was clear: the current system was inadequate, and new architecture was needed.

Outputs and Continuity

By the end of Day 1, the groups had produced a list of concrete proposals:

- Single Due Diligence Digital Badge
- Financial Common Operational Picture (FIN COP)
- SME compliance passports and guarantees
- Reform of MoD payment protocols
- Defence banking consortium with government backing
- Reframing ESG to include Security

- Creation of a Shadow Ministry of Economic Warfare

These outputs were not neat or final, but they were tangible. More importantly, they reflected the lived frustrations and creative ideas of those directly engaged in defence finance and innovation.

On Day 2, almost all of these proposals reappeared in the formal conference debates. The hackathon had succeeded in surfacing the raw material for policy.

As one participant observed in closing, ***"Yesterday we aired the frustrations. Today we begin to turn them into action."***

CENTRE FOR ECONOMIC SECURITIES

DAY 2
FORMAL CONFERENCE

Day 2 of the Future of Security Conference shifted from experimentation to strategy. Where Day 1 had been raw, candid, and exploratory, Day 2 was deliberate, structured, and strategic. The attendees were more senior — leaders from major banks, defence primes, technology firms, and government agencies. The setting was formal, though still under Chatham House rules, ensuring frankness without attribution.

The continuity was intentional. The frustrations and proposals of Day 1 were not discarded but explicitly used to frame the Day 2 agenda. As the chair reminded the audience at the outset, ***"Yesterday we saw the system through the eyes of those living it. Today we decide what to do about it."***

Opening Plenaries: Setting the Strategic Frame

The morning opened with plenary interventions from senior figures in academia, government, and the armed forces. The message was stark: the UK is already in an economic war.

One keynote framed it bluntly: ***"For eighty years, peace was the assumption. That assumption is over. We face adversaries who use every lever — finance, law, property, food, culture, technology — to weaken us. This is not competition. This is conflict."***

Another speaker stressed the centrality of economic resilience: ***"You can't deter if you can't endure. Factories, farms, and fibre are as decisive as tanks and planes."*** A former military commander went further: ***"Our adversaries know we can fight. They doubt we can last. The test is not whether we have forces on day one, but whether we can sustain them on day one thousand."***

One delegate, speaking from long experience, warned of the cost of delay: ***"History teaches us that democracies prefer to wait until the emergency is undeniable. By then it is too late. Self-preservation strikes its jarring gong only when the damage is done."***

This framing shaped the day's debates. The task was no longer to diagnose whether economic warfare existed, but to decide how to respond.

Finance & Institutional Reform

The first major theme was finance. The outputs of Day 1 loomed large. Participants noted the banks' reluctance to fund defence SMEs and the structural barriers of compliance, ESG, and reputational risk. ***"Money is the fastest weapon we have,"*** one speaker declared, ***"but right now, it is locked in the armoury."***

Several proposals were debated in depth:

- Defence & Infrastructure Finance Charter: a co-developed charter between government, banks, and industry to define the rules of engagement for defence finance. It would clarify risk-sharing, embed ESG+Security as a guiding principle, and create channels for blended finance such as critical infrastructure bonds.
- Banking consortium: a group of major banks pooling resources to fund defence, backed by government guarantees to reduce exposure.
- Loss Absorption & Resilience Fund: a mechanism to de-risk strategic projects by underwriting potential losses, making it easier for banks to engage.
- SME Compliance Passport: a streamlined credential to replace repeated, duplicative checks and give SMEs predictable access to finance.

These proposals were explicitly linked to Day 1 outputs. The Single Due Diligence Badge and FIN COP concepts were referenced as prototypes that could be developed further.

Underlying these technical debates was a broader cultural question: how to shift finance from short-term profitability to long-term security. ***"Profit, compliance, and security objectives currently clash,"*** one banker admitted. "***We need political signals to reconcile them."***

Innovation & Risk Culture

The second theme was innovation. Here too, Day 1 frustrations reappeared in elevated form. SMEs had complained of risk aversion, bureaucratic inertia, and the privileging of process over performance. On Day 2, senior leaders acknowledged this as a systemic flaw.

"We have created a culture where failure is punished, conformity is rewarded, and risk is avoided," one participant observed. ***"That is the opposite of what a preparedness economy requires."***

The discussion emphasised the need for:

- Trial-and-error experimentation: enabling rapid prototyping, testing, and iteration rather than endless approval processes.
- Dual-use technology: fostering innovation in AI, cyber, and data that can serve both civilian and defence needs.
- Blended finance models: combining public guarantees with private investment to fund high-risk, high-reward technologies.
- Tolerance of failure: embedding cultural change in both government and finance

SME Ecosystem Strengthening

The third theme was SMEs. The voices of Day 1 SMEs echoed in the room, quoted back by senior participants. The payment delays, the lack of credit, the risk-averse banking culture — all were recognised as systemic threats.

One senior defence figure warned: ***"SMEs are not subcontractors to primes. They are strategic assets in their own right. Lose them, and we lose resilience."***

Proposals included:

- Government-backed working capital guarantees for SMEs engaged in defence.
- Reform of MoD payment protocols to provide earlier milestone payments.
- Creation of long-term banking relationships with SMEs, not one-off project loans.
- Greater transparency and fairness in prime-SME partnerships, avoiding dependence that replicates state fragility with private monopoly.

The principle was clear: SMEs must be seen as essential nodes in the security ecosystem, not disposable suppliers.

Supply Chain Resilience

The fourth theme was supply chains. Day 1 had raised concerns about single sourcing, clustering, and just-in-time fragility. Day 2 deepened the analysis. Speakers noted that the UK's supply chains are opaque beyond the first tier, leaving critical dependencies hidden until crisis strikes. ***"We know who supplies us,"*** one participant said, ***"but we don't know who supplies them."***

Proposals included:

- Mapping supply chains to the raw material level.
- Diversifying sources geographically and sectorally.
- Building surge capacity domestically to replace imports in crisis.
- Stress-testing industries against disruption scenarios.

- Funding redundancy by design to avoid single points of failure.

The debate recognised the costs. Redundancy is inefficient in peacetime terms. But the consensus was clear: "Resilience is expensive, but fragility is fatal."

Offensive Economic Statecraft

The fifth theme was perhaps the most provocative. Most Western debates focus on defensive resilience. But several speakers insisted that credible deterrence requires offensive tools.

Examples included:

- Digital blockades: restricting adversaries' access to key networks, platforms, and data flows.
- Financial disinformation campaigns: undermining adversary confidence in their own institutions and markets.
- Bloc-scale wartime protocols: harmonising NATO and EU measures for sanctions, liquidity, and payments.
- Contraband seizure: updating historical practices for the digital age, seizing illicit data or transactions.

The argument was simple: without offensive capacity, deterrence collapses. As one participant put it, "Defence alone invites pressure. Only offence creates deterrence."

The National Economic Security Centre

Throughout the day, the idea of a Ministry of Economic Warfare resurfaced. On Day 1, it had been sketched as a provocative experiment. On Day 2, it was treated as an urgent necessity.

The Ministry idea has evolved into a core recommendation which is to establish a National Economic Security Centre. This Centre would provide clarity, accountability, and coordination. It would integrate finance, trade, intelligence, and technology policy. It would liaise with allies and serve as a single point of contact for industry. Such a National Economic Security Centre could be replicated at Nato or EU level to ensure that the activities of sovereigns were coordinated under Article 2 or Strategic Autonomy provisions, for example.

Some raised concerns about duplication or bureaucracy. But the prevailing mood was that existing institutions are too fragmented and too slow. ***"We do not need another strategy document,"*** said one senior participant. ***"We need an institution that can act at crisis speed."***

Closing Consensus

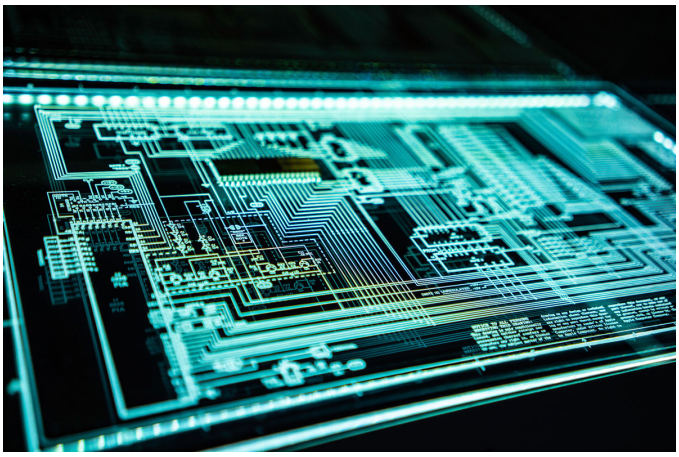
By the end of Day 2, several consensus points had emerged:

1. The UK is already engaged in economic warfare. Delay is dangerous.
2. Economic resilience is as decisive as military strength.
3. Government must send clear signals to banks and industry.
4. SMEs are strategic assets and must be supported accordingly.
5. Data integration is essential to overcome silos.
6. Institutions must be permanently adaptable, not episodically reviewed.

7. Offensive as well as defensive tools are required.

The atmosphere was one of sober urgency. Participants recognised the scale of the challenge but also the possibility of alignment. The continuity from Day 1 to Day 2 was clear: the raw frustrations of SMEs and banks had been translated into policy debates; the experimental proposals of the hackathon had become strategic recommendations.

As the conference closed, one participant summed up the mood: ***"We have diagnosed the disease. Now we must take the medicine. Waiting is no longer an option."***



CROSS-CUTTING THEMES & CONTINUITY

The design of the Future of Security Conference — a bottom-up hackathon on Day 1 followed by a formal, high-level policy conference on Day 2 — revealed clear lines of continuity. The candid frustrations and proposals of Day 1 were not left behind; they were elevated into strategic conversations on Day 2. This deliberate sequencing allowed for a rare bridging of perspectives: those who experience systemic obstacles daily, and those with the power to reshape the system.

The cross-cutting themes that emerged across both days can be grouped into five broad areas: government signalling and legitimacy, SMEs as strategic assets, the role of finance, data and intelligence integration, and the balance between centralisation and decentralisation.

1. Government Signalling and Legitimacy

One of the strongest continuities was the demand for clear political signals from government. On Day 1, bankers repeatedly emphasised their reluctance to finance defence SMEs without cover. ***"We need the fig leaf from government,"*** one said. The reputational risks, ESG misalignments, and shareholder pressures were simply too great to face alone.

On Day 2, senior participants echoed this theme. Without a clear, bipartisan signal that financing defence is a public good and a national priority, banks will hesitate. As one speaker put it, ***"Profit, compliance, and security currently clash. Only government can reconcile them."***

This theme highlights the legitimacy gap. Defence finance is not just about capital flows; it is about the moral and political framing of what constitutes legitimate investment. By embedding Security into ESG, creating charters, and sending consistent signals, government can shift the risk calculus for finance.

2. SMEs as Strategic Assets

A second theme was the fragility yet indispensability of SMEs. On Day 1, SMEs voiced their struggles: cash flow crises, compliance burdens, exclusion from credit. Their frustration was palpable. ***"We are expected to deliver national security with no oxygen,"*** one complained.

On Day 2, these voices were amplified. Senior figures explicitly recognised SMEs as strategic assets. ***"SMEs are essential nodes in the ecosystem,"*** said one defence leader.

The continuity here is significant. Day 1 framed the SME plight in operational terms; Day 2 reframed it as a strategic vulnerability. The result was a consensus that SMEs must be supported with guarantees, compliance passports, and reformed payment protocols.

3. The Role of Finance

Finance was the thread running through both days. On Day 1, banks laid out their obstacles; SMEs vented their frustrations; technologists demanded transparency. Out of this came ideas like the Single Due Diligence Badge and FIN COP.

On Day 2, these ideas were elevated into proposals for a Defence & Infrastructure Finance Charter, banking consortia, and resilience funds. The technical details varied, but the underlying continuity was clear: finance is both the bottleneck and the potential accelerator of a preparedness economy.

The debates showed the contradiction at the heart of finance: the pursuit of short-term profit versus the necessity of long-term security. Both days acknowledged that this cannot be resolved by banks alone. It requires government guarantees, shared risk mechanisms, and cultural change.

4. Data & Intelligence Integration

Data silos emerged as a theme on Day 1, especially from the technology group. ***"The problem is not what we don't know, but what we can't access,"*** one participant said. The idea of FIN COP was born directly from this frustration.

On Day 2, the same idea appeared in elevated form. Senior participants discussed integrating financial flows, supply

chain risks, and threat intelligence into a common picture. Without such integration, decisions are made in the dark.

The continuity here is the recognition that information asymmetry is a systemic vulnerability. Whether in finance, supply chains, or compliance, the absence of a shared operational picture creates inefficiency and fragility. Both days agreed that overcoming this requires secure, structured, real-time intelligence sharing across sectors.

5. Centralisation vs. Decentralisation

A final theme was the tension between centralisation and decentralisation. On Day 1, SMEs called for autonomy, faster payments, and less dependence on primes. Tech companies demanded more freedom to innovate. Banks wanted clearer government direction. Government itself admitted to fragmentation.

On Day 2, this became a debate about institutional design. Should resilience come from centralised institutions like a Ministry of Economic Warfare, or from dispersed, redundant ecosystems of SMEs and innovators? The answer, most agreed, was both.

As one participant summarised, ***"We need centralisation for strategy and decentralisation for resilience. Scale for the big platforms, slack for the fragile links."***

This theme reflects a broader truth of economic warfare: efficiency without redundancy is vulnerability; decentralisation without coordination is chaos. The balance must be struck deliberately.

Additional Threads

Several other cross-cutting insights deserve mention:

- Redundancy vs. Efficiency: Both days emphasised that peacetime efficiency creates wartime fragility. ***"Resilience is expensive, but fragility is fatal,"*** became a refrain.
- Trial and Error: Day 1 SMEs and technologists demanded room to experiment. Day 2 leaders echoed this as a systemic need. ***"We must work by trial and error, not error and trial."***
- Offence as Deterrence: Day 1 floated provocative ideas about offensive tools. Day 2 developed them into a policy agenda. The continuity here was the recognition that deterrence requires the credible capacity to impose costs.

From Candid Frustration to Policy Agenda

The greatest achievement of the two-day structure was its continuity. Day 1 exposed raw frustrations: banks paralysed by reputational risk, SMEs gasping for credit, technologists blocked by silos, government mired in inertia. Day 2 transformed those frustrations into structured debates and policy proposals.

This continuity built trust. Participants could see their concerns reflected and elevated. The banker who complained about reputational risk on Day 1 saw the idea of a Defence Finance Charter debated on Day 2. The SME who demanded ***"stop telling us what we can't do"*** saw milestone payment reforms on the agenda. The technologist who called for FIN COP heard senior leaders endorse the idea.

The bridge between days was not just rhetorical; it was substantive. The hackathon surfaced the pain points, and the formal conference converted them into strategic direction.

Conclusion of Themes

In sum, the cross-cutting themes of the Future of Security Conference highlight a convergence:

- Government must provide signals and frameworks.
- SMEs must be treated as strategic assets.
- Finance must be unlocked as a weapon.
- Data must be integrated into shared pictures.
- Institutions must balance centralisation with decentralisation.

The continuity between Day 1 and Day 2 ensured that this convergence was not imposed from above but built from below. The frustrations of practitioners became the priorities of leaders.

As one participant reflected in closing, ***"The genius of these two days is that we heard the truth from the floor and then debated it at the top. If we can now act with the same continuity, we might yet prepare in time."***

POLICY RECOMMENDATIONS & ACTIONS

The two days of the Future of Security Conference generated not only analysis and debate but also a coherent set of policy recommendations. These recommendations were not drawn up in isolation by experts, nor imposed top-down by government, but emerged from the continuity of frustration, dialogue, and consensus across a diverse set of constituencies. They represent the beginnings of a blueprint for a preparedness economy in an era of economic war.

The following actions were identified as priorities:

1. Reframe Defence as a Public Good

A recurring theme was the need to shift the cultural and political framing of defence. At present, defence is often perceived as a cost, a reputational risk, or an ethical compromise. ESG frameworks, shareholder activism, and public opinion frequently treat defence as inconsistent with social or environmental goals.

The recommendation was clear: defence must be reframed as a public good, essential for societal resilience and economic prosperity. ***"Security is the first human right,"*** one participant said. ***"Without it, there is no prosperity, no sustainability, and no freedom."***

This reframing would involve:

- Embedding "Security" explicitly within ESG, creating ESG+S frameworks.
- Public communication strategies emphasising defence as enabler of civil society.
- Clear, bipartisan political statements affirming the legitimacy of defence finance.

By doing so, government provides banks and investors with the political cover they need to finance defence confidently.

2. Defence & Infrastructure Finance Charter

Day 2 discussions crystallised around the idea of a Defence & Infrastructure Finance Charter, co-developed by government, banks, and industry. This would establish agreed principles for financing national security, including:

- Risk-sharing mechanisms (e.g., partial guarantees).
- Clear ESG+S standards.
- Channels for blended finance such as infrastructure bonds.
- Transparency to reassure shareholders and regulators.

Such a charter would allow banks to act collectively rather than individually exposed. It would normalise defence finance as legitimate and structured, reducing the reputational risks that dominate today.

As one banker put it, ***"Give us the framework and we can provide the capital. Without it, we will hesitate and delay."***

3. SME Support and Empowerment

SMEs emerged as both fragile and indispensable. Supporting them requires tailored instruments:

- Compliance passports: a once-and-done credential to replace duplicative due diligence checks.
- Working capital guarantees: government-backed instruments to prevent cash flow crises.
- Reformed MoD payment protocols: milestone-based payments to ensure SMEs are not starved of cash.
- Fair partnerships with primes: transparency and oversight to prevent exploitative subcontracting.

One SME put it starkly: ***"We cannot deliver national security if we are permanently on life support."*** The consensus was that

SMEs should be recognised as strategic assets, not incidental suppliers. Supporting them strengthens resilience, innovation, and redundancy across the economy.

4. Intelligence & Data Integration

The lack of shared intelligence was repeatedly identified as a systemic vulnerability. Solutions proposed included:

- Financial Common Operational Picture (FIN COP): a secure platform integrating data on finance, supply chains, and threats across government, banks, and industry.
- Single Due Diligence Digital Badge: standardising compliance checks across all lenders and regulators.
- Data-sharing protocols: creating secure mechanisms for private-public intelligence exchange.

"The problem is not what we don't know, but what we can't access," said one technologist. This recommendation directly addresses that asymmetry.

5. Institutional Reform: National Economic Security Centre

Perhaps the most striking recommendation was the call for a Ministry (or Shadow Ministry) of Economic Warfare, which has been operationalised in this report through the concept of a National Economic Security Centre. Its purpose would be to:

- Integrate policy across finance, trade, intelligence, and industry.
- Serve as a single point of contact for banks, SMEs, and tech firms. Partnership, indeed collaboration between government, corporate and financial players is the DNA of the new defence-technological-financial complex and this also needs to be in the DNA of the Ministry of Economic Warfare.
- Coordinate offensive and defensive economic tools.
- Liaise with allies to align measures and share intelligence.
- Possess delegated crisis authority to act at speed.

Critics worried about duplication or bureaucracy. But most participants saw the status quo as worse: fragmented, slow, and unaccountable. The Ministry would not replace existing departments but would serve as a permanent hub for economic statecraft.

6. Supply Chain Resilience

Both days highlighted the fragility of current supply chains. Recommendations included:

- Mapping supply chains to raw-material levels.
- Diversifying suppliers geographically and sectorally.
- Building domestic surge capacity for critical industries.
- Funding redundancy and stockpiles by design.
- Stress-testing sectors against disruption scenarios.

This requires accepting inefficiency in peacetime. "***Resilience is expensive, but fragility is fatal,"*** became a refrain. The shift from just-in-time to just-in-case supply chains is costly but unavoidable.

7. Foster Innovation & Risk Culture

Cultural change was as important as structural reform. Participants urged a shift from risk aversion to risk tolerance:

- Encourage rapid prototyping and trial-and-error methods.
- Accept failure as a necessary cost of innovation.
- Use blended finance to support dual-use technologies.
- Create fast-track approval channels for experimental projects.

Only by fostering risk-taking can the UK hope to keep pace with adversaries who adapt rapidly.

8. Offensive Economic Statecraft

Defensive resilience is insufficient. Deterrence requires offensive capacity. Recommendations included:

- Designing digital blockades to restrict adversary access to networks and platforms.
- Deploying financial disinformation campaigns to erode adversary confidence.
- Developing bloc-wide wartime protocols for sanctions, payments, and liquidity.
- Modernising contraband seizure for the digital age.

As one voice insisted, "***Defence alone invites pressure. Only offence creates deterrence.***"

This recommendation was among the most controversial but also the most urgent. Without credible offensive tools, adversaries will exploit Western restraint.

9. Whole-of-Society Mobilisation

The final recommendation was holistic: mobilising the entire society for preparedness. This means:

- Educating citizens honestly about the risks.
- Building resilience into civil infrastructure.
- Integrating private sector, academia, and civil society into security planning.
- Establishing standing joint bodies with delegated crisis authority.

War today is not fought by armies alone. It is fought across economies, societies, and infrastructures. A preparedness economy requires whole-of-society engagement.

As one participant summarised, "***Security is not a sector. It is the condition of everything else.***"

Recommendations

The policy recommendations of the Future of Security Conference are ambitious but coherent. They demand institutional reform, financial innovation, cultural change, and societal mobilisation. Above all, they require urgency.

The conference consensus was clear: the UK is already in an economic war. Delay will guarantee reactive, fragmented, and chaotic responses. By acting now — reframing defence, supporting SMEs, integrating intelligence, reforming institutions, securing supply chains, fostering innovation, developing offensive tools, and mobilising society — the UK can build resilience and deterrence. ***"We have diagnosed the disease,"*** one participant concluded. "***Now we must take the medicine. The time for analysis is over.***

The time for execution is now."

The Future of Security Conference closed with a powerful sense of urgency. Across two days — one experimental, one strategic — participants converged on a shared recognition: the UK is already engaged in an economic war. This is not a metaphor, nor a distant prospect. It is a daily reality in the financial system, in supply chains, in cyberspace, and in the political economy of global interdependence.

The challenge is immense. The institutions, financial systems, and industrial base of the UK remain optimised for peacetime efficiency, not wartime resilience. The assumption that economic interdependence would guarantee peace has been shattered. Adversaries exploit that interdependence as a weapon. In this environment, resilience is not a luxury but a precondition for survival.

CONCLUSION
FROM ANALYSIS TO EXECUTION

Day 1 laid bare the frustrations of those on the frontlines of this reality: SMEs suffocated by cash flow crises, banks paralysed by reputational risk, technologists blocked by data silos, government trapped in inertia. Their voices were candid, sometimes angry, but always constructive. Out of this candour emerged practical innovations: compliance passports, digital badges, common operational pictures, financial consortia, and the provocative idea of a Ministry of Economic Warfare.

Day 2 elevated those frustrations into strategic debates. Senior leaders confronted the stark reality: deterrence requires endurance, endurance requires resilience, and resilience requires reform. They debated finance charters, supply chain redundancy, offensive economic tools, and cultural change. They recognised SMEs as strategic assets, reframed defence as a public good, and acknowledged that government must send clear signals to legitimise defence finance.

The continuity between the two days was striking. What began as frustration became strategy. What emerged as raw proposals became policy recommendations. The hackathon surfaced pain points; the conference transformed them into actionable directions. This structure ensured that the voices of practitioners informed the decisions of leaders — a rare bridging of perspective that built trust and credibility.

The themes were clear:

- Government must lead with signals and frameworks.
- Finance must be unlocked as a weapon, not left paralysed by reputational fear.
- SMEs must be empowered as indispensable nodes of resilience.
- Intelligence and data must be integrated to overcome silos.
- Institutions must combine centralisation for strategy with decentralisation for resilience.
- Resilience must be funded, even at the cost of peacetime efficiency.
- Offensive as well as defensive tools are required for deterrence.
- Preparedness is a whole-of-society endeavour.

The path forward is difficult, but the alternative is worse. Delay will guarantee a reactive, fragmented, and chaotic response when crisis strikes. Democracies cannot afford to wait until the emergency is undeniable. As one participant observed, ***"Self-preservation strikes its jarring gong only when the damage is done."***

The task now is to move decisively from analysis to execution. That means creating the institutions, charters, and frameworks recommended. It means accepting the costs of resilience. It means empowering SMEs, mobilising finance, and integrating intelligence. It means preparing society for uncertainty and disruption. Above all, it means acting with urgency.

As the conference closed, one voice captured the sentiment of the room: ***"If you can't make it, move it, or fix it when it breaks, you don't own it — your adversary does."***

The Future of Security Conference did not just diagnose the problem. It offered the beginnings of a cure. The responsibility now lies with government, finance, industry, and society to take the medicine — and to act before it is too late.

CONTACT

ABOUT THE CENTRE FOR ECONOMIC SECURITY

The Centre for Economic Security is a research and convening organisation that dedicates itself to three goals: first, raising awareness and understanding of economic threat, second, to establishing the operational tools to manage that threat and third to enabling policy makers, financial institutions and corporates to anticipate and deal strategically with those threats.

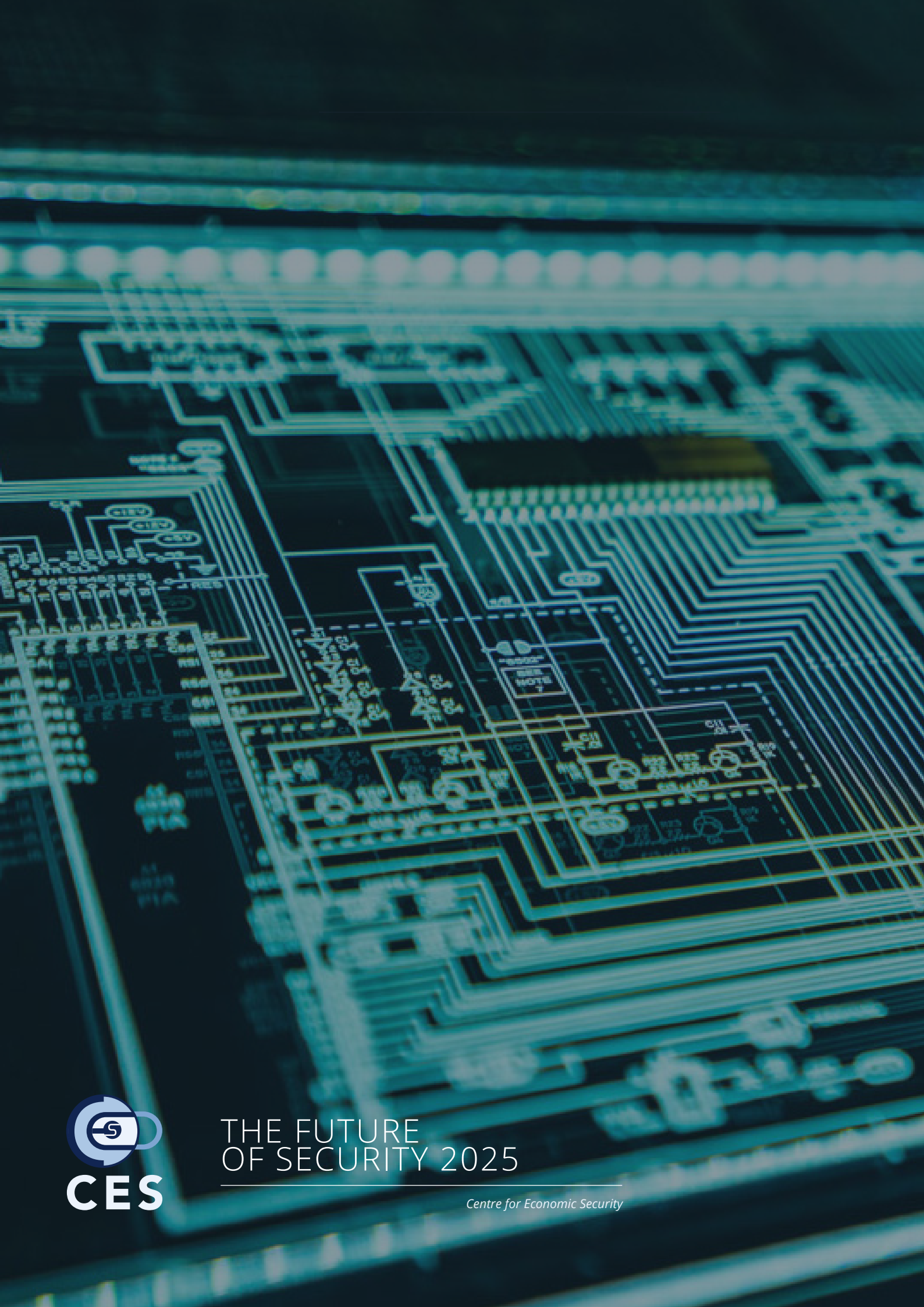
Our vision is to promote strategic economic readiness in a fragmented world. We do this by working with governments, financial institutions and corporates to formulate resilient and effective tools.

CONTACT

Dr. Rebecca Harding, CEO
Dr. Jack Harding, Head of Research

info@ces-global.net
ces-global-net

Design by W'A.I



CES

THE FUTURE OF SECURITY 2025

Centre for Economic Security