CENTRE FOR ECONOMIC SECURITY

FUTURE OF SECURITY 2026

THE BUSH HOUSE AGREEMENT

The Articles and Delivery Architecture of Productive Security

Core proposition

Preparedness is created through productive ecosystems.

Full Report — Revised Working Draft v3

Derived from the Future of Security Conference, Bush House, King's College London, 29–30 June 2026

Prepared by the Centre for Economic Security

August 2026

Status and evidential basis

This working draft develops the Articles of Productive Security agreed through the Future of Security process into a full explanatory and implementation report. Its evidential boundary is the conference record: the Day One and Day Two transcripts, table notes, emergency injects, audience questions and voting files. Consultation feedback is used to refine and clarify the Agreement, but not to manufacture retrospective consensus. Subsequent CES research and institutional development are identified separately as work derived from the Bush House mandate.

The conference was held under the Chatham House Rule. Accordingly, arguments are reported without attributing remarks to individual participants unless the material was already delivered as a public keynote or separately published. Transcript references identify the day and timecode for auditability rather than the speaker.

Contents

Executive summary

The Bush House Agreement begins from a simple but consequential proposition: the security of an open society depends upon its ability to create, finance, sustain and adapt the productive capabilities on which national security, democratic resilience and prosperity depend. Economic security is therefore not a peripheral concern of trade or industrial policy. It is the economic foundation of national power and the means through which societies prepare for, withstand and respond to both human-generated and natural threats.

The Future of Security Conference was designed as a negotiation rather than a conventional policy event. Ten thematic tables examined climate, food, energy and water, macroeconomics and regulation, finance, civil society, trade and supply chains, defence resilience, defence transition, cyber security, and space, artificial intelligence and emerging technologies. Participants were required to move beyond diagnosis and negotiate a smaller number of institutions capable of connecting government, industry, finance, technology, academia and civil society. The process reduced ten table proposals to five priority institutions and then reframed them as components of a common system.

The evidence from the day is unusually clear. Participants repeatedly concluded that the problem was not necessarily a shortage of institutions, capital or expertise, but the absence of common direction, shared visibility and mechanisms capable of acting across silos. The five final institutions—the Investment Compact, ASTA, the Defence Security and Resilience Bank, the Public Information Institute and COBRA with teeth—represented strategic leadership, intelligence, finance, innovation and public legitimacy, connected through a practical coordination function. The vote did not establish six equivalent ecosystems. It established five bodies of capability that required an integrating operating system.

The architecture

Ten Articles define the principles. Five delivery ecosystems organise the capabilities. CES provides the independent threat-detection, coordination and operational interface that turns those capabilities into action.

The ten Articles constitute the Agreement's normative core: Security through Productive Capability; Growth through Resilience; Connected Ecosystems; Strategic Visibility; Mobilising Capital; Innovation and Adaptation; Preparedness; Democratic Resilience; Allied Prosperity; and Continuous Learning. Together they define Productive Security as the ability of an economy and society to generate and adapt productive capability for national security and long-term prosperity.

Delivery is organised through five ecosystems: Strategic Leadership; Strategic Intelligence and Systemic Risk; Financial Resilience; Innovation and Productive Capability; and Societal and Democratic Resilience. CES acts as independent steward and operates the cross-cutting economic-security coordination function described at Bush House as "COBRA with teeth". Its role is to detect threats, assess their consequences, connect government and industry, convene the relevant capabilities, develop response options, coordinate action, escalate material risks, monitor delivery and embed learning.

This approach does not seek to replace markets with central direction. Bush House recognised both the strategic value of open markets and their exposure to coercion, concentration, opacity and short-term incentives. The Agreement therefore addresses strategic market failure: circumstances in which commercial decisions may remain individually rational while the system fails to create the capabilities, redundancy, finance or information required for collective security. Intervention must be disciplined, proportionate and transparent about costs. Resilience is not costless; preparedness involves choices over who pays, who benefits, which risks deserve priority and which capabilities must be retained before their value is commercially visible.

The work undertaken after Bush House begins to provide the transmission mechanisms. CES's economic-security research explains the relationship between markets, power and strategic market failure. The blended-finance work explains how public commitments, guarantees, multilateral finance, private capital, trade finance, supply-chain finance and receivables finance can translate strategic priorities into bankable investment and productive liquidity. Security Returns on Investment provides a route to measuring whether that finance generates capability, resilience, growth and public value.

1. From Future of Security 2025 to Bush House 2026

The Bush House Agreement is the second stage of a conversation that began at the inaugural Future of Security Conference on 23–24 July 2025. The 2025 event brought defence and security SMEs, banks and finance providers, technology and data companies, government representatives, academics and practitioners together to examine why the UK remained poorly configured for economic conflict. Day One used a hackathon format to expose operational barriers; Day Two translated those barriers into a strategic policy agenda. The central conclusion was that economic endurance depends on productive capability, finance, supply chains, data and public legitimacy as much as on military assets.

The 2025 discussion was anchored explicitly in defence. Banks described the political, compliance and reputational barriers to financing defence SMEs. SMEs described cash-flow pressure, slow procurement and dependence on prime contractors. Technology companies identified data silos, while government participants acknowledged fragmented responsibility. The result was a practical agenda: reframe defence as a public good; create a Defence and Infrastructure Finance Charter; provide working-capital guarantees

and simpler due diligence for SMEs; develop a Financial Common Operational Picture; map and diversify supply chains; fund redundancy and surge capacity; and create a central economic-security coordination capability.

The National Economic Security Centre was already present in this first agenda. The 2025 report and ministerial briefing proposed a centre modelled functionally on the National Cyber Security Centre, capable of identifying economic threats, connecting government with finance and industry, coordinating allies and supporting crisis response. The phrase "When everyone owns it, no one owns it" captured the institutional problem. The purpose of the centre was to provide ownership of coordination without centralising every delivery function.

2025 foundation	Development at Bush House in 2026
Defence as a public good and a productive investment	Articles I, II and VIII connect capability, growth and democratic legitimacy.
Defence and Infrastructure Finance Charter; working-capital guarantees	Financial Resilience and Blended Finance Ecosystem.
FIN COP, trusted data networks and supply-chain mapping	ASTA, OSEINT and the Strategic Intelligence and Systemic Risk Ecosystem.
National Economic Security Centre	CES as the independent threat-detection and government–industry interface.
Supply-chain redundancy, surge capacity and SME support	Innovation and Productive Capability Ecosystem.
Whole-of-society preparedness and public narrative	Societal and Democratic Resilience Ecosystem.

Bush House 2026 therefore did not start again. It widened the frame from defence finance and economic warfare to Productive Security across defence, infrastructure, climate, food, water, energy, finance, communications, technology and civil society. More importantly, it negotiated how the capabilities identified in 2025 should be connected. The Bush House Agreement is the constitutional and delivery architecture for that continuing programme.

2. Why Bush House was necessary

2.1 The economy as a strategic domain

The conference record describes an international system in which economic interdependence is no longer assumed to be benign. Trade, finance, technology, data, logistics, energy and commodity markets have become instruments through which power is exercised. States and private actors can exploit chokepoints,

standards, subsidies, ownership structures, market concentration, data control and supply-chain dependencies without crossing the threshold into conventional conflict. At the same time, climate disruption, extreme weather, pandemics, cyber incidents and infrastructure failure can weaken the same productive systems without a hostile actor being present.

This convergence matters because the effects propagate across domains. A climate shock can reduce transport capacity, raise food prices, disrupt health systems and create political instability. A technology restriction can halt industrial production and affect both civilian and military capability. A disruption to shipping, payments or insurance can turn an operational event into an economy-wide liquidity problem. The conference therefore resisted treating defence, food, energy, climate, finance, digital infrastructure and civil society as separate security conversations.

2.2 From efficiency to preparedness

Participants repeatedly returned to the consequences of optimising systems for efficiency without valuing redundancy, adaptability or recovery. The problem was not efficiency itself, but the assumption that stable conditions would persist and that markets would always be able to source substitutes quickly. Deep-tier suppliers, critical raw materials, telecommunications, space infrastructure, payments, insurance and logistics were all identified as areas in which apparently efficient arrangements could conceal single points of failure.

Preparedness was therefore proposed as the organising principle of economic security. This is an all-hazards proposition. The capabilities required to identify vulnerable people, maintain communications, finance continuity, map dependencies and mobilise suppliers may be useful across a pandemic, flood, cyberattack, blockade or war. Investment before a crisis can be less costly than improvised action after capability has disappeared, but the Agreement also recognises that such investment must be prioritised and its benefits made visible.

2.3 Strategic market failure

The subsequent CES economic-security work gives a precise name to the problem exposed at Bush House. Strategic market failure occurs when markets operate according to prevailing commercial incentives yet fail to produce or preserve capabilities essential to long-term security and resilience. It can arise from information gaps, time-horizon mismatches, unpriced systemic risk, external dependencies, coordination failures, fragmented demand signals or the inability of smaller suppliers to finance scale and working capital.

Strategic market failure does not mean that every strategic sector should be protected or publicly owned. It means that the market outcome must be evaluated against the capability required under conditions of

disruption. The relevant policy question is not whether the state or the market should act in the abstract, but which combination of regulation, procurement, guarantees, finance, information-sharing, convening and international cooperation is proportionate to a defined risk.

3. From negotiation to Agreement

3.1 The negotiating process

Day One asked ten tables to define their principal vulnerabilities, identify institutional or regulatory responses and negotiate practical recommendations. Two tables were explicitly focused on defence resilience and defence transition, while defence requirements also ran through the finance, trade, technology and supply-chain discussions. Crisis injects tested whether proposals could respond to changing conditions. Participants were then instructed to negotiate the ten proposals into five connected institutional functions.

3.2 The five functions before the vote

The first function was strategic direction. The Investment Compact, developed from the finance discussion, would align government, financial institutions, industry, national security and civil society around strategic investment priorities and the meaning of fiduciary responsibility in a less secure world. It supplied the proposed system with agenda-setting, policy coherence and long-term demand signals.

The second was strategic intelligence and technological visibility. ASTA emerged from the space, AI and emerging-technology table, but its scope widened during negotiation. It would map supply chains and technology dependencies, combine open-source and trusted commercial information, identify innovation opportunities and provide an accelerator and procurement bridge. It was both a diagnostic engine and a link between evidence, innovation and finance.

The third was a financial ecosystem. Defence participants called for rapid and agile capital, particularly working capital for SMEs and finance for alternative or allied supply chains. Finance participants stressed that the UK did not lack capital so much as the pipes, investable propositions and shared direction required to deploy it. The DSRB was explicitly proposed as one multilateral mechanism, but the negotiated function was broader: a connected escalator spanning trade and supply-chain finance, guarantees, private credit, commercial banks, institutional capital, sovereign mechanisms and multilateral finance.

The fourth was societal legitimacy. The Public Information Institute was proposed as an independent, two-way interface with citizens and civil society. Its role was not to amplify threat messages, but to ensure that public experience shaped policy and that the economic, community and distributional consequences

of preparedness were understood. Without that legitimacy, long-term defence and resilience commitments would not survive political cycles.

The fifth was operational coordination. COBRA with teeth described a cross-silo public–private function able to turn warning into decision and decision into delivery. It connected the strategic direction of the Compact, the evidence generated through ASTA, the financing ecosystem and the societal interface. The conclusion of the negotiation was that the five should not compete as isolated institutions: they needed to operate as one system.

3.3 What the votes established

The first multi-selection poll showed the strongest support for ASTA, followed by an empowered DSRB and COBRA with teeth. The final single-selection poll then ranked the five negotiated institutions. These results should not be read as a mandate to implement only the highest-ranked body. The transcript records that the five had absorbed the principal functions emerging from all ten tables and that delegates wanted the option to endorse the ecosystem as a whole.

Final institution	Votes	Share	Function carried into the Agreement
ASTA — Alliance for Security Technology Advantage	23	33%	Strategic intelligence, supply-chain visibility and innovation
COBRA with teeth	13	19%	Cross-silo coordination, rapid response and government–industry interface
Defence Security and Resilience Bank	13	19%	Financial resilience and mobilisation of public and private capital
Public Information Institute	12	17%	Public legitimacy, trusted communication and civil-society participation
Capital Markets Challenge Board / Investment Compact	8	12%	Strategic leadership, fiduciary alignment and investment direction

The final architecture developed in this report therefore preserves the substance of the vote while avoiding a false hierarchy. Five delivery ecosystems hold the capabilities represented by the five institutions. CES provides the coordinating function necessary for them to operate as a system.

3.4 Consultation and finalisation

Consultation responses broadly validated the Productive Security framing while asking for greater precision on implementation, climate and nature security, defence capability, infrastructure, skills, data ownership, bankability, international cooperation and democratic legitimacy. The strongest critique was

that broad principles can conceal real trade-offs. The full report responds by defining each Article, stating the problem it addresses and setting out the choices, responsibilities and measures required for delivery.

4. Productive Security defined

Definition

Productive Security is the ability of an economy and society to create, finance, sustain and adapt the productive capabilities required for national security, democratic resilience and long-term prosperity.

The definition contains five elements. “Create” recognises the importance of innovation, enterprise, infrastructure and skills. “Finance” recognises that capability is not operational unless firms can invest, scale and fund working capital. “Sustain” recognises maintenance, redundancy, trusted supply and continuity. “Adapt” recognises that threats, technologies and markets change. “Productive capabilities” places the emphasis on real economic capacity rather than expenditure alone.

Productive Security is not synonymous with self-sufficiency. No open economy can or should reproduce every input domestically. The goal is managed interdependence: understanding dependencies, identifying where substitution or redundancy is necessary, maintaining trusted partnerships and ensuring that the economy can respond at the speed required. Nor is Productive Security confined to defence. Defence credibility depends on energy, food, water, communications, logistics, finance, skills, health, public legitimacy and critical social infrastructure.

4.1 The intellectual architecture of the five ecosystems

The five ecosystems are not an arbitrary re-labelling of the institutions proposed at Bush House. They reflect an intellectual argument developed across Rebecca Harding’s conference interventions and subsequent papers: security depends on the interaction of strategic direction, intelligence, finance, productive capacity and democratic consent. Like Keynes’s institutional work around Bretton Woods, the purpose is to translate an analysis of systemic failure into durable machinery for cooperation and delivery. The Articles state the principles; the ecosystems organise the capabilities; CES turns both into an operating programme.

A Bretton Woods Moment for Productive Security explains why today’s productive-capacity gap is principally a problem of institutional architecture and capital allocation. It supports the connected-ecosystem model and the need for OSEINT-led coordination across national capability, critical national infrastructure and critical social infrastructure. Towards a Defence Spending Model shows why expenditure commitments alone do not create capacity: defence SMEs and supply chains require working

capital, guarantees, credible demand and blended public–private finance. This anchors defence explicitly within the Financial Resilience and Innovation ecosystems.

Multilateral Finance: Securing the Scalability and Competitiveness of UK Defence demonstrates the distinct functions of procurement coordination, sovereign risk-sharing, national finance and longer-duration multilateral capital. It supports a modular funding escalator in which no single proposed institution is indispensable. Economic Power and National Security: A New Framework for Blended Finance develops the transmission mechanism: strategic market failure is corrected through productive liquidity, a blend of procurement, guarantees, export credit, private capital, trade and receivables finance, and potentially a Sovereign Productive Security Fund. Together these papers explain both why the five ecosystems are appropriate and why their next phase must be institution-building rather than further diagnosis.

5. The ten Articles of Productive Security

Article I — Security through Productive Capability

Economic security shall be understood as the capability of a society to create, finance, sustain and adapt the productive capacity upon which prosperity, resilience, preparedness and national security ultimately depend.

This Article establishes productive capability as the foundation of security. It directs attention away from headline expenditure and towards whether the economy can deliver useful capacity: firms, people, infrastructure, technology, finance and supply networks. Its implementation requires capability mapping, clear demand signals and attention to deep-tier suppliers.

Article II — Growth through Resilience

Investment in resilient infrastructure and productive capability should be recognised as investment in innovation, competitiveness and long-term economic growth. Economic security should therefore be assessed as productive investment, while its costs and opportunity costs remain transparent.

The Article preserves the conference's growth-through-resilience proposition while acknowledging the consultation challenge. Some resilience investments generate immediate productivity benefits; others purchase insurance against disruption. Both require appraisal, but the absence of a conventional short-term return does not imply an absence of economic value.

Article III — Connected, Whole-of-System Ecosystems

Economic security cannot be achieved through isolated institutions or individual sectors. It requires coherent, whole-of-system ecosystems linking government, finance, industry, technology, academia and civil society through shared objectives, responsibilities and principles of engagement.

The record repeatedly identifies fragmentation as the central institutional failure. Connection must extend beyond networking: participants need rules for information-sharing, escalation, decision rights and accountability. This Article provides the basis for the five delivery ecosystems and CES coordination function.

Article IV — Strategic Visibility, Ownership and Control

Information is strategic infrastructure. Trusted visibility, appropriate ownership and control, secure access and proportionate portability across supply chains, financial systems, technologies, infrastructure, assets and dependencies are essential to preparedness and collective decision-making.

Visibility is not equivalent to indiscriminate disclosure. The conference identified commercial sensitivity, national-security restrictions and foreign ownership as constraints. The objective is a governed information architecture that combines open-source intelligence, anonymised commercial data and protected channels.

Article V — Mobilising Bankable Capital

Public and private capital should be mobilised to strengthen productive capability, accelerate innovation and build long-term resilience. This requires investable propositions, commercially credible returns, policy certainty and proportionate public risk-sharing where markets cannot carry strategic risk alone.

This Article is made operational by the Financial Resilience Ecosystem. It recognises that capital cannot be commanded into unbankable projects. Public institutions must create credible pipelines and use guarantees, procurement, catalytic finance and data to reduce uncertainty while preserving commercial discipline.

Article VI — Innovation, Skills and Adaptation

Innovation, entrepreneurship, skills, leadership and technological capability are strategic assets. Economic security depends upon conditions in which new capabilities can flourish and scale while trusted markets, intellectual property, democratic values and allied competitiveness are protected.

The conference emphasised agility and the ability to respond to technologies or threats not yet known. Universities, SMEs, entrepreneurs, investors, established firms and public procurement must therefore form an adaptive capability system rather than a linear innovation pipeline.

Article VII — Preparedness

Preparedness should become the organising principle of economic security policy across human-generated and natural threats. Government, industry, finance and civil society should build and exercise productive capability before crises emerge.

This Article moves the system from reactive crisis management to continuing preparedness. It requires scenario exercises, maintained response options, pre-agreed financing channels, supplier visibility and mechanisms capable of moving rapidly when warning thresholds are crossed.

Article VIII — Democratic and Societal Resilience

Public confidence, trusted information, democratic legitimacy and tangible community benefit are strategic capabilities. Citizens and civil society must participate in the diagnosis, choices and distributional consequences of preparedness.

The conference recognised that threat communication alone cannot create legitimacy. Public support depends on credibility, value for money, visible local and economic benefits, and honesty about winners, losers and opportunity costs. Democratic resilience is therefore a condition of implementation, not a communications afterthought.

Article IX — Allied Prosperity and Managed Interdependence

Economic resilience is strengthened through trusted partnerships among allies and partner nations. Shared capability, coordinated investment, resilient supply networks, collaborative innovation and open markets should support security while managing critical dependencies.

No national architecture can resolve systemic dependencies alone. Cooperation nevertheless requires clarity about trust, burden-sharing, procurement, information protection and the possibility that partners may act differently in extremis.

Article X — Continuous Learning and Accountability

Economic security is a continuous process of learning, innovation and institutional evolution. The Agreement commits participants to exercises, pilots, measurement, independent review and adaptation as technologies, markets and threats change.

This Article prevents the Agreement from becoming a static declaration. CES's stewardship, annual Bush House review and publication of implementation assessments provide the principal learning and accountability cycle.

6. The five delivery ecosystems

The ecosystems are not new bureaucratic silos. Each is a function-led network that combines existing organisations and, where necessary, new mechanisms. Their boundaries are deliberately permeable because threats move across them. CES provides the common operating and escalation layer.

Ecosystem	Purpose	Bush House reference points
Strategic Leadership	Align national priorities, investment, fiduciary expectations and policy across strategic sectors and infrastructure.	Investment Compact / Capital Markets Challenge Board
Strategic Intelligence and Systemic Risk	Create shared visibility of geopolitical, climate, technological, financial, supply-chain and societal risks.	ASTA, OSEINT and governed data-sharing
Financial Resilience and Blended Finance	Translate strategic priorities into bankable finance from SMEs and working capital to national and multilateral investment.	Investment Compact; blended-finance and financing escalator
Innovation and Productive Capability	Connect research, skills, entrepreneurs, firms, procurement, finance and infrastructure to create and scale capability.	ASTA's accelerator and productive-capability functions
Societal and Democratic Resilience	Build public legitimacy, trusted information, participation, education, community benefit and preparedness.	Public Information Institute and civil society

6.1 Strategic Leadership Ecosystem

The Strategic Leadership Ecosystem establishes shared direction without assuming that every participant has the same incentives or duties. Its role is to define priority risks, agree principles of engagement, identify where fiduciary and national-resilience objectives intersect, and create credible long-term signals for investors and industry. The Investment Compact is the principal Bush House reference point: a public–private leadership mechanism connecting financial institutions, government, national security, industry and civil society.

6.2 Strategic Intelligence and Systemic Risk Ecosystem

This ecosystem supplies the common operating picture. It combines open-source economic intelligence, commercial and financial signals, supply-chain and asset mapping, technology assessment, climate and nature intelligence, and protected government information where appropriate. ASTA is its principal institutional anchor. Climate is treated as a systemic threat multiplier rather than a subsidiary environmental issue, connecting extreme weather, food, water, health, infrastructure, logistics and displacement.

6.3 Financial Resilience and Blended Finance Ecosystem

The Financial Resilience and Blended Finance Ecosystem begins with the defence problem made explicit in both years of the conference: military and dual-use capability cannot scale if SMEs cannot finance payroll, inventory, production, certification and delivery while waiting for procurement milestones or payment. Working capital is therefore a security capability. Trade finance, supply-chain finance, receivables finance, purchase-order finance, guarantees and private credit are as strategically important to productive mobilisation as long-term project capital.

The ecosystem connects the full funding escalator. At firm and supply-chain level this includes commercial banks, specialist lenders, insurers, trade-finance providers, primes and private credit. At national level it includes procurement authorities, export credit agencies, the British Business Bank, the National Wealth Fund, pension funds, insurers and a potential Sovereign Productive Security Fund. At allied and multilateral level it may include partner-country institutions and the Defence, Security and Resilience Bank.

The DSRB remains in the report because it was explicitly discussed and endorsed at Bush House. It should not, however, be presented as an institution owned, directed or guaranteed by CES. Its future now sits principally with governments, including the Canadian government, and is politically contingent. Within the Agreement it is therefore one possible multilateral instrument in a wider financing ecosystem—not the ecosystem's anchor and not a dependency of CES delivery.

The Investment Compact supplies the strategic interface: it aligns demand, policy and fiduciary expectations and helps create a pipeline of credible opportunities. Blended finance supplies the transmission mechanism: public procurement, first-loss or guarantee capacity and catalytic institutions allocate risks that markets cannot carry alone, while private investors retain commercial discipline. The practical test is whether the architecture turns commitments into bankable propositions and gets productive liquidity to firms at the time it creates capability.

6.4 Innovation and Productive Capability Ecosystem

This ecosystem turns research and enterprise into deployable capacity. It connects universities, technology accelerators, SMEs, primes, infrastructure operators, skills providers, venture and growth capital, procurement bodies and allied partners. It also preserves the broader technological and commercial base needed to respond to unexpected developments. Innovation is therefore assessed not only by invention, but by time to productive capability, ability to scale, trusted supply and operational relevance.

6.5 Societal and Democratic Resilience Ecosystem

The Societal and Democratic Resilience Ecosystem places citizens at the centre of preparedness. It connects civil society, consumer organisations, communities, educators, behavioural expertise, media and creative industries with government and business. Its task is two-way: to ensure that public experience informs decision-making and that preparedness choices are explained credibly. The Public Information Institute is a mechanism for trust and participation, not a vehicle for top-down messaging.

7. A National Economic Security Centre: turning "COBRA with teeth" into an institution

"COBRA with teeth" was the phrase used by participants to describe the practical capability they believed was missing: a public–private agility and coordination function able to connect intelligence, finance and industry quickly enough to act. The 2025 report had already proposed a National Economic Security Centre modelled functionally on the National Cyber Security Centre. Bush House 2026 supplied the negotiated ecosystem architecture within which that centre could operate. The two propositions should now be brought together.

Institutional proposition

CES should develop and operate an independent National Economic Security Centre function: the threat-detection engine, government–industry–finance interface and operational steward of the five Bush House ecosystems.

The analogy with the National Cyber Security Centre is functional rather than constitutional. The NCSC sits within government and GCHQ; CES does not. CES should not claim government authority, access to classified intelligence or command over public bodies. Its comparative advantage is independence: it can combine OSEINT, ASTA-style technology and supply-chain intelligence, commercial signals, financial evidence and practitioner networks, and then translate that evidence between national-security institutions and the firms and financiers expected to act.

Capability	Operational meaning
Detect	Maintain continuing visibility of threats, dependencies, market signals and capability gaps.
Assess	Evaluate consequences for government, industry, finance, infrastructure, communities and allies.
Connect	Operate a trusted interface between government and the private sector, translating security sensitivities into usable economic decisions.

Capability	Operational meaning
Convene	Bring together the relevant ecosystem participants before and during a crisis.
Develop options	Translate intelligence into financial, industrial, regulatory, technological, trade and communications responses.
Coordinate	Align action and remove bottlenecks without displacing statutory or commercial responsibilities.
Escalate	Ensure material threats and failures reach institutions with the authority or resources to act.
Monitor	Track preparedness, commitments and implementation gaps; publish independent assessments.
Learn	Use exercises, incidents, pilots and annual reviews to strengthen the system continuously.

The “teeth” must therefore be institutional rather than rhetorical. CES requires access to relevant data, standing relationships across the five ecosystems, agreed warning and escalation protocols, the ability to form time-limited task groups, and a published mechanism for following recommendations through to implementation. Independence is essential because the interface must be trusted across political parties, government departments, commercial competitors and civil society.

The immediate development path is deliberately practical. CES can begin externally to government by building the OSEINT and ASTA threat-detection engine, establishing sector liaison and escalation networks, running exercises and pilots, and publishing independent preparedness assessments. Formal government recognition or access can deepen the model later, but the Centre’s initial value does not depend on being created by statute or absorbed into Whitehall.

8. Choices, costs and trade-offs

8.1 Resilience is not costless

The Agreement does not assume that preparedness and short-term efficiency always reinforce one another. Redundancy, stockpiles, diversified sourcing, domestic capacity, cyber protection, infrastructure adaptation and maintained skills can impose current costs. Resources committed to resilience cannot simultaneously fund every other public or commercial objective. The case for intervention must therefore specify the risk, the capability required, the probability and consequence of failure, and the distribution of costs and benefits.

8.2 A prioritisation test

A practical prioritisation framework should examine: strategic relevance; severity and timing of the threat; concentration and substitutability; time required to restore capability; spillovers across sectors; public and distributional consequences; feasibility and cost of mitigation; allied alternatives; and the risk that intervention itself creates dependency, protectionism or moral hazard. CES should publish the methodology and distinguish evidence from judgement.

8.3 Division of labour

Government should define national objectives, set law and regulation, use procurement and guarantees where public authority is required, and protect classified information. Industry should identify operational constraints, invest and deliver under commercially credible conditions. Finance should price and allocate capital while making clear which risks cannot be carried privately. Academia and technology organisations should generate evidence and innovation. Civil society should shape legitimacy, distributional choices and public preparedness. CES should connect these responsibilities, expose gaps and escalate unresolved coordination failures.

8.4 Markets and openness

The purpose of Productive Security is to protect the adaptive and informational value of open markets, not to normalise indiscriminate economic nationalism. Measures that restrict trade, ownership, data flows or competition must be necessary, proportionate and reviewable. Allied sourcing, diversification, standards cooperation and targeted risk-sharing will often be preferable to self-sufficiency. Where protected capability is required, its costs and exit conditions should be explicit.

9. Governance and implementation

9.1 Stewardship

CES will steward the Agreement on behalf of the wider Bush House community. Stewardship includes maintaining the Articles, convening the five ecosystems, operating the coordination function, monitoring progress and publishing implementation assessments. The Agreement itself remains a shared framework rather than the property of any single government, party or commercial interest.

9.2 Participation and endorsement

Endorsement signifies support for the principles of the Articles; it does not constitute a legally binding commitment or automatic approval of every illustrative institution. Conference endorsement,

consultation support, organisational signatory status and governmental endorsement should be recorded separately. This distinction allows broad participation without overstating institutional authority.

9.3 First implementation cycle

1. Establish a CES Bush House steering group and terms of reference for the five ecosystems.
2. Publish the threat, vulnerability and prioritisation methodology used by the coordination function.
3. Run a COBRA-with-teeth pilot focused on a defined trade, supply-chain or financing disruption.
4. Develop a governed ASTA/OSEINT common operating picture and escalation protocol.
5. Map the financial escalator from working capital and trade finance to sovereign and multilateral investment.
6. Develop the Public Information Institute model with civil-society participation from inception.
7. Publish baseline indicators and an annual Bush House implementation assessment.

10. From Agreement to action

Work undertaken after the conference is included here as evidence of implementation and intellectual development, not as retrospective evidence of what delegates agreed. Its status should be stated explicitly in all future editions.

10.1 Economic security, markets and power

The subsequent economic-security paper develops the intellectual foundation of the Agreement. It explains how economic conflict changes the operation of markets; how price signals can be distorted by coercion, concentration, strategic subsidies and uncertainty; and why protecting market democracy requires institutions capable of identifying and correcting strategic market failure. This work deepens Articles I–IV and clarifies why Productive Security is a framework for economic power as well as resilience.

10.2 Blended finance as a transmission mechanism

The blended-finance work develops Article V into a practical financial architecture. Traditional blended finance uses public or catalytic resources to mobilise private capital where market failures inhibit socially valuable investment. In the Productive Security context, its role expands: it reduces strategic uncertainty, turns long-term commitments into investable propositions and creates productive liquidity throughout critical supply chains.

The architecture includes public procurement and guarantees, export credit, commercial and institutional capital, private credit, trade finance, supply-chain finance and receivables finance. A Sovereign Productive Security Fund can accelerate access to cash against approved future receivables rather than waiting for slow payment cycles. The DSRB may provide one multilateral layer if participating governments take it

forward, while national institutions and commercial markets provide sectoral and firm-level finance. The objective is not subsidy without discipline; it is to allocate risk to the institutions best able to carry it and to ensure that strategic projects offer credible commercial returns.

10.3 Security Returns on Investment

Security Returns on Investment provides a prospective measurement framework for finance and policy. It can assess whether an intervention creates additional productive capability, reduces dependency, improves substitutability, preserves skills, accelerates time to productive capability, strengthens supply-chain resilience or generates wider economic and social benefits. This work responds directly to conference questions about how resilience should be measured and valued.

10.4 CES as the National Economic Security Centre

The evolution of CES towards an economic-security threat-detection and coordination centre is the institutional consequence of Bush House. The centre's research, OSEINT/data capability, financial architecture work, convening role and public-facing legitimacy work provide the foundations. The next stage is to turn these elements into standing protocols, pilots, escalation pathways and transparent accountability.

11. Measures of progress

No single ratio can measure Productive Security. The first measurement framework should combine capability, preparedness, finance, resilience, legitimacy and learning. Indicators should be few enough to govern decisions, but sufficiently disaggregated to avoid concealing fragility.

Dimension	Illustrative measures
Strategic visibility	Coverage of critical supply tiers and assets; warning lead time; unresolved data gaps.
Productive capability	Time to productive capability; surge capacity; skilled workforce; domestic and allied substitutability.
Financial resilience	Capital mobilised; leverage of catalytic funds; SME working-capital access; financing speed and additionality.
System resilience	Concentration, redundancy, recovery time, exercised continuity plans and cross-sector dependencies.
Innovation	Progression from research to procurement; scale-up finance; trusted IP and allied technology collaboration.

Dimension	Illustrative measures
Democratic legitimacy	Public confidence, distribution of local benefits, transparency of trade-offs and civil-society participation.
Institutional performance	Threats assessed, options developed, bottlenecks resolved, recommendations implemented and lessons adopted.

The wake-up call

The two Future of Security conferences produced the same warning by different routes. In 2025, defence SMEs, banks, technology firms and government representatives exposed a system that could identify its weaknesses but struggled to finance or correct them. In 2026, a wider group negotiated the institutions required to connect those capabilities. The gap is no longer primarily conceptual. It is operational.

Economic conflict, military mobilisation, climate disruption, technological concentration and supply-chain coercion do not wait for institutional tidiness. A state that cannot see its dependencies, communicate with industry, finance its suppliers or retain public legitimacy cannot create credible deterrence. A strategy without productive capacity is an aspiration; a procurement commitment without working capital is not capability; intelligence without a route to decision is only observation.

Wake-up call

The warning from Bush House is not that the next crisis may expose these weaknesses. It is that the weaknesses are already being used. The task now is to build the National Economic Security Centre, connect the five ecosystems and move from agreement to operational preparedness.

CES next steps: from Agreement to delivery

The closing interventions on Day Two were unequivocal. Rebecca Harding called for structures that hold the ideas together, communicate their public value, measure economic-security threats and mobilise capital across defence, cyber, food, energy and space. Richard Wardlaw argued for focus, political engagement, white papers, taskforces and the institutions required before conflict—not after it. Greg Kennedy called for a campaign plan, allies, people, messages and practical support for CES to perform the institution-building role. CES will convert that mandate into the following immediate programme.

Immediate actions — first 90 days

1. Publish the final Bush House Agreement, a consultation response and an evidence map linking every Article and ecosystem to the conference record, while identifying subsequent research separately.
2. Constitute a CES Bush House Steering Group and five ecosystem taskforces, each with a named chair, terms of reference, a delivery partner map and one defined first-year output.
3. Publish the operating proposition for an independent National Economic Security Centre, including governance, safeguards, liaison arrangements, warning thresholds, escalation routes and the boundary between independent analysis and government authority.
4. Build the first OSEINT/ASTA common operating picture: a governed threat taxonomy and initial dashboard covering selected trade, supply-chain, technology and financial indicators.
5. Convene an Investment Compact and blended-finance design roundtable to select a demonstrator pipeline and map the complete funding escalator from SME working capital and productive receivables to institutional, sovereign-backed and possible multilateral finance.
6. Begin the communications campaign proposed at the conference: a letter to the administration, a public or Financial Times intervention, and a cross-party open letter ahead of the party-conference cycle.

Delivery actions — within six months

1. Run a “COBRA with teeth” pilot against a defined disruption affecting defence or critical infrastructure, bringing government-facing, industry and finance participants together around warning, options, capital and execution; publish an unclassified after-action review.
2. Launch a short CES white-paper series—one paper for each ecosystem—showing its instruments, networks, decision rights, dependencies and first practical use case.
3. Develop the blended-finance demonstrator into an investable proposition, testing guarantees, contract and receivables finance, private credit and Security Returns on Investment without making delivery dependent on the DSRB or any single political decision.
4. Establish standing liaison networks across priority sectors and allied partners, including finance, defence, communications, food, energy, technology and civil society, so warnings can reach people able to act.
5. Secure the people and resources required for delivery through a transparent CES membership, partnership and funding plan that protects analytical independence.

Accountability — within twelve months

1. Publish the first Productive Security baseline and Bush House scorecard, covering strategic visibility, time to productive capability, financing speed, supply-chain resilience, innovation, democratic legitimacy and implementation.
2. Reconvene the Bush House community to review progress, test the five ecosystems through a further scenario and agree the next implementation cycle.
3. Report publicly against each commitment: completed, in progress, delayed or superseded, with named ownership and an explanation of material barriers.

The immediate commitment

CES will move first on the functions within its control: convening the five taskforces, specifying the National Economic Security Centre, building the OSEINT/ASTA prototype, designing the financial demonstrator and publishing the evidence and accountability framework. Government recognition and multilateral instruments can strengthen delivery, but CES action will not wait for them.

Closing declaration

The Bush House Agreement reflects a shared understanding that the security of open societies depends not only on their capacity to defend themselves, but on their ability to create productive, innovative, legitimate and resilient economies. Its purpose is not to create additional bureaucracy. It is to provide a common framework through which government, industry, finance, technology, academia and civil society can prepare together.

The Agreement establishes ten Articles of Productive Security, five delivery ecosystems and an independent CES coordination function. It recognises that preparedness requires investment, choices and accountability; that markets remain essential but cannot resolve every strategic coordination failure unaided; and that national capability is strongest when built through trusted allied relationships and democratic consent.

The commitment

Preparedness is created through productive ecosystems. The Bush House Agreement therefore marks not the conclusion of a conference, but the beginning of a continuing programme of collaboration, implementation and learning.

Appendix A — Evidence hierarchy

Evidence class	Use in this report
Votes and formally agreed conclusions	Establish the negotiated mandate and priority institutional functions.
Day One and Day Two transcripts	Establish arguments, areas of consensus, tensions and the evolution of the architecture.
Table notes and audience questions	Capture detailed proposals, sectoral concerns and unresolved questions.
Conference briefings and crisis injects	Establish the designed negotiating context and tests applied to proposals.
Consultation feedback	Refine language and identify implementation requirements without rewriting the event record.
Subsequent CES work	Demonstrate development and implementation arising from the mandate.

Appendix B — Voting record

The final Day One poll recorded 69 votes across the five negotiated institutions: ASTA 23; COBRA with teeth 13; DSRB 13; Public Information Institute 12; and Capital Markets Challenge Board 8. An earlier multi-selection poll, reported in the complete export, recorded particularly strong support for ASTA, COBRA with teeth and the DSRB. Variation between interim exports is retained in the audit files; the final single-selection poll is the authoritative record for institutional ranking.

Appendix C — Glossary

Term	Definition
All-hazards preparedness	Capabilities and arrangements designed to operate across natural, technological, economic and hostile threats rather than for one scenario alone.
ASTA	Alliance for Security Technology Advantage: the Bush House proposal for technology, supply-chain and strategic-dependency intelligence combined with innovation and acceleration functions.
Blended finance	The strategic use of public, catalytic or guarantee capacity alongside private capital to allocate risk, create bankable propositions and mobilise investment.
COBRA with teeth	The participant-generated description of a cross-silo public–private function able to turn warning into options, coordination and implementation. In this report it develops into the National Economic Security Centre proposition.

Term	Definition
Critical National Infrastructure (CNI)	Assets, systems and networks whose disruption would have serious consequences for essential services, national security, public safety or the economy.
Critical Social Infrastructure	The institutions, services and community systems—including health, education, food access and trusted information—on which societal functioning and democratic resilience depend.
Defence, Security and Resilience Bank (DSRB)	A proposed multilateral financing institution for defence, security, resilience and dual-use capability. It is treated here as one potential instrument within a wider financing ecosystem.
Economic security	The ability of a society to protect and sustain the economic systems, capabilities and relationships on which sovereignty, prosperity, resilience and national security depend.
Financial Common Operational Picture (FIN COP)	The 2025 proposal for a trusted shared view of financial flows, supply-chain exposure and relevant threat information across government, finance and industry.
Funding escalator	The connected range of financing instruments required as firms and projects move from working capital and early-stage finance through scale-up, institutional and multilateral capital.
Managed interdependence	An approach that preserves the benefits of open markets while identifying, diversifying and governing dependencies whose disruption would create unacceptable strategic risk.
National Economic Security Centre (NESC)	The proposed independent CES function that detects and assesses economic-security threats, bridges government with industry and finance, coordinates the five ecosystems and monitors preparedness.
OSEINT	Open-Source Economic Intelligence: the systematic collection and assessment of public and commercially shareable information to identify economic threats, vulnerabilities, dependencies and opportunities.
Preparedness economy	An economy that invests, coordinates and exercises capabilities before crises occur rather than relying primarily on improvised response.
Productive liquidity	Finance delivered at the time and through the instrument required to create, accelerate or preserve real productive capability.
Productive Security	The ability of an economy and society to create, finance, sustain and adapt the productive capabilities required for national security, democratic resilience and long-term prosperity.
Security Returns on Investment	A framework for assessing the additional economic, societal and security outcomes created by finance or policy, including capability, resilience, dependency reduction and preparedness.
Strategic market failure	A condition in which market participants respond rationally to commercial incentives but the resulting system fails to create or preserve capabilities essential to long-term security and resilience.

Term	Definition
Time to productive capability	The time required for finance, investment or intervention to produce a usable operational capability rather than merely approve expenditure.

Endnotes

1. Centre for Economic Security and King's College London ECCRG, The Future of Security 2025: Event Summary, October 2025.

2. Centre for Economic Security, National Economic Security Centre: Future of Security Conference Outcomes and Policy Recommendations, ministerial briefing, October 2025.

3. Future of Security Conference, Day One transcript, 29 June 2026, 00:37:33–00:38:52 (need for a financial ecosystem and coordination across economic-security threats).

4. Ibid., 01:01:12–01:02:58 (preparedness as a shared societal responsibility and the requirement to move from analysis to action).

5. Ibid., 02:48:41–02:50:29 and 06:06:26–06:07:50 (capital availability, the absence of a whole-system approach and the proposed capital-markets convening function).

6. Ibid., 02:59:52–03:00:19 (the proposal for a COBRA with teeth including public and private sectors).

7. Ibid., 05:58:42–06:01:43 (climate risk as system-level risk and the need to unblock capital flows).

8. Ibid., 06:30:51–06:31:24 and 07:31:46–07:37:28 (reduction to five frameworks and the conclusion that they should operate as an ecosystem).

9. Ibid., 06:44:30–06:45:27 and 07:23:46–07:30:36 (identification of the five final institutions and their connected functions).

10. Future of Security Conference, Day Two transcript, 30 June 2026, 00:11:33–00:14:34 (the Bush House Agreement as the framework for continuing work).

11. Ibid., 01:02:33–01:06:16 (five coordinating and delivery functions, including COBRA economics, ASTA, the DSRB and the Public Information Institute).

12. Polls Overall—Future of Security 2026, complete export, Day One final poll, 29 June 2026.

13. Future of Security 2026, Table Note Takers, defence transition and resilience notes, 29 June 2026.

14. Future of Security Conference, audience questions, 30 June 2026 (measurement and valuation of resilience, beneficial finance and market pricing of long-term risk).

15. Centre for Economic Security, The Bush House Agreement: Draft Articles of Productive Security, version 4, July 2026.

16. Bush House Agreement consultation documentation, July–August 2026.

17. Rebecca Harding, “A Bretton Woods Moment for Productive Security”, Rebeccanomics, July 2026, https://rebeccanomics.com/commentary/bretton-woods-productive-security/.

18. Rebecca Harding, “Towards a Defence Spending Model”, Rebeccanomics, July 2026, https://rebeccanomics.com/commentary/towards-a-defence-spending-model/.

19. Rebecca Harding, “Multilateral Finance: Securing the Scalability and Competitiveness of UK Defence”, Rebeccanomics, June 2026, https://rebeccanomics.com/commentary/multilateral-finance-uk-defence-scalability/.

20. Rebecca Harding, “Economic Power and National Security: A New Framework for Blended Finance”, Rebeccanomics, August 2026, https://rebeccanomics.com/commentary/blended-finance-productive-security/.

21. Future of Security Conference, Day Two transcript, 30 June 2026, 06:49:00–07:10:00 (closing interventions by Rebecca Harding, Richard Wardlaw and Greg Kennedy on communication, institution-building, political engagement, taskforces, resources and immediate action).