Review of the UK National Security Strategy 2025: What Happens Next?

Published: Ambient Stratagem

June 2025

Executive Summary

The National Security Strategy 2025 represents the most significant reformulation of the United Kingdom's strategic doctrine since the end of the Cold War. It does not merely react to the proliferation of threats, but articulates a systemic response to an increasingly hostile and ambiguous global operating environment. It accepts, with rare clarity, that the United Kingdom is now engaged in persistent contestation with peer adversaries whose methods fall deliberately below the threshold of open war [1]. In doing so, the Strategy marks the official entry of the British state into what adversaries have long understood as the Grey Zone [3][4][5].

At its core, NSS 2025 signals a decisive shift from a risk management model toward a campaigning mindset. The government formally recognises that national security must now be approached as a whole-of-state effort, with the homeland no longer insulated from threat. This includes the prospect of wartime conditions on UK soil, a conclusion that emerges not from speculative analysis, but from the cumulative observation of adversary doctrine and behaviour [1][3].

Russia, China, and Iran are all explicitly identified as actors engaging in sustained hybrid activity against the United Kingdom and its allies. Their methods, cyber attacks, infrastructure probing, political interference, disinformation and proxy operations align with established strategic frameworks: Russia's theory of reflexive control [3], China's Three Warfares and systems confrontation doctrine [4], and Iran's use of asymmetrical deniability through non-state actors [5]. NSS 2025 demonstrates a clear-eyed understanding of these methods, and acknowledges the growing operational convergence between them [1].

Strategic Transformation Vectors

In response, the Strategy sets out a coherent transformation of British statecraft across five critical vectors:

Operational Readiness at Home

The UK formally prepares for hostile activity against the homeland, including sabotage, cyber intrusion, and attacks on critical national infrastructure. Maritime security operations such as Operation Atlantic Bastion, and the modernisation of border enforcement and territorial surveillance, reflect an understanding that domestic sovereignty can no longer be assumed, it must be actively secured [1].

Infrastructure as a Strategic Domain

NSS 2025 reclassifies the infrastructure environment as a contested battlespace. Undersea cables, energy pipelines, ports, and data centres are recognised not only as economic assets but as targets for coercion and disruption. The Strategy embraces this logic and extends defensive responsibilities accordingly [1][3].

Integration of AI, Cyber, and Electromagnetic Warfare

The establishment of a unified Cyber Electromagnetic Command and the commitment to build an AI-enhanced, highly lethal force by 2035 reflect a doctrinal realignment. The UK now views software-defined capability, decision-speed, and spectrum dominance as essential instruments of national power and essential to parity with adversaries that already embed these layers into their campaigns [1][2][4].

Grey Zone Literacy and Strategic Realism

The Strategy reveals a matured view of modern conflict. It rejects outdated binaries between war and peace, recognising instead a state of continuous competition. It acknowledges the strategic collusion between peer adversaries across multiple theatres and positions the UK to act with agility, reciprocity, and when necessary, outside traditional multilateral frameworks [1][5].

National Security as Economic Statecraft

Perhaps most significantly, NSS 2025 fuses economic policy with national defence. A 5 percent GDP commitment to security is framed not as an obligation, but as an engine for renewal [2]. Defence investment is positioned to regenerate industrial capacity, attract private capital into sovereign technologies, and align domestic prosperity with international resilience [1].

Across these domains, the Strategy is not only reactive, it is anticipatory. It accepts that the adversarial playbook is already in use, and designs a national posture that seeks not just to deter aggression, but to shape the environment in which such aggression occurs. The campaigning language adopted throughout the Strategy is deliberate. It denotes a long-term, multi-domain approach that views security as an evolving contest rather than a fixed state.

This white paper offers a doctrinal analysis of the strategic shift embodied in NSS 2025. It traces the trajectory from resilience to readiness, maps the infrastructure and cyber domains as active theatres, evaluates the integration of AI and electromagnetic warfare into UK force design, and calibrates the Strategy against the operational logics of the United Kingdom's most capable adversaries.

The central finding is this: the UK is now structurally engaged in a sustained Grey Zone conflict. The question is not whether this has begun, it has. The question is whether the institutional, industrial and strategic alignment necessary to prevail can be delivered with the required coherence, tempo and legitimacy.

References

1. National Security Strategy 2025, CP 1338, HM Government, 24 June 2025
2. Reuters, "UK to broaden security focus, set 5% defence spending target", 23 June 2025
3. MOD SDR 2025, Section 3.4, "Hybrid and Reflexive Adversary Threats", 2 June 2025
4. Financial Times, "UK identifies China's systems confrontation doctrine", 24 June 2025
5. AP News, "Iran's asymmetric playbook targeting the UK", 23 June 2025

1. From Resilience to Readiness

The National Security Strategy 2025 begins with an unmistakable shift in posture: a recognition that the defensive crouch of recent decades is no longer sufficient to preserve British security, prosperity, or sovereignty. Resilience, once regarded as the principal objective of national preparation, is recast as a necessary but incomplete state. In its place comes readiness, not as a measure of capacity in isolation, but as a posture of mobilisation across the political, economic and societal spectrum [1].

The Strategy acknowledges that the United Kingdom now operates in an environment shaped by persistent pressure from adversarial state and non-state actors. The security assumptions that once underpinned domestic policy, that national infrastructure would remain inviolate, that international rules would regulate strategic competition, and that geography offered insulation from conflict, no longer hold. In their place, the government outlines a campaign-based approach to security, accepting the reality of long-term engagement in contested space and affirming that national power must be structured accordingly [1].

This doctrinal shift is anchored in a fundamental reappraisal of threat. The Strategy names Russia as the most acute and immediate danger to the Euro-Atlantic order, citing its use of sub-threshold activity, cyber operations, nuclear coercion, and sabotage against the United Kingdom and its allies [1]. It highlights the expanding influence of Iranian intelligence networks, operating on British soil with the intent of intimidating diaspora communities, disrupting public discourse, and degrading internal cohesion [5]. And it notes that hostile state activity is no longer limited to espionage or isolated attacks, but increasingly embedded in the fabric of everyday life, often via criminal proxies, digital platforms and infrastructure exploitation [1][5].

The document is unequivocal: the UK must now prepare for the possibility of a wartime scenario within its own borders [1]. This is not a return to Cold War-era civil defence, nor a speculative contingency. It is a reflection of observed adversarial behaviour, combined with a sober projection of the UK's exposure to hybridised forms of aggression. In this context, readiness is not measured in deployments or inventories alone. It is defined by the state's ability to preserve decision-making coherence, operational tempo, and infrastructural integrity under conditions of strategic disruption.

To support this posture, the Strategy outlines a programme of investment, capability reform, and cultural adaptation. The commitment to raise national security spending to 5 percent of GDP by 2035 is more than a fiscal target [2]. It represents a structural repositioning of security within the machinery of government, industry, and public expectation. Importantly, it is accompanied by a mandate for systemic change, one that prioritises cross-government planning, integrates civilian and military responses, and moves beyond the assumption that resilience alone can deter coercion [1].

This new approach draws on lessons from peer adversary doctrine. The UK's strategic planners now recognise that Russia's reflexive control model [3], China's systems confrontation doctrine [4], and Iran's persistent deniability strategy [5] are designed to operate beneath formal thresholds, while still achieving coercive effect. These models depend not on superior firepower, but on the ability to outpace, confuse and fragment. The Strategy responds by emphasising strategic clarity, public unity, and infrastructural control, all elements which adversaries have explicitly targeted in recent years [1].

Operational readiness, as defined in NSS 2025, begins with the defence of territory. The establishment of enhanced maritime operations to counter undersea threats, the modernisation of the UK's border command structures, and the renewed emphasis on sabotage protection within national infrastructure are not isolated measures. They are the early contours of a wider effort to restore credibility to the idea of deterrence by denial, a posture that does not seek escalation, but which refuses to cede space to adversarial pressure [1].

Alongside these hard measures, the Strategy also places emphasis on narrative integrity and public understanding. It accepts that in the Grey Zone, public perception is a strategic terrain in its own right. The government's commitment to increasing public awareness of national threats, launching annual resilience exercises, and integrating preparedness into public education reflects a growing understanding that national coherence is not a by-product of security, it is a precondition for it [1].

What emerges is a posture that does not regard readiness as a static condition, but as an institutional habit. It is a posture that recognises the need to generate and sustain tempo across government, military, intelligence, industry, and civil society. It accepts the reality that the adversary is already campaigning. The question, therefore, is whether the state is configured to do the same, not merely to manage risk, but to shape the environment in which risks manifest [3] [4].

In this sense, National Security Strategy 2025 should be read not simply as a new chapter in British defence policy, but as the beginning of a strategic transformation, one that reintroduces national preparedness as a sovereign obligation, revalidates deterrence in an age of ambiguity, and reorients the British state to act with coherence under pressure.

References

1. National Security Strategy 2025, CP 1338, HM Government, 24 June 2025
2. Reuters, "UK to broaden security focus, set 5% defence spending target", 23 June 2025
3. MOD SDR 2025, Section 3.4, "Hybrid and Reflexive Adversary Threats", 2 June 2025
4. Financial Times, "UK identifies China's systems confrontation doctrine", 24 June 2025
5. AP News, "Iran's asymmetric playbook targeting the UK", 23 June 2025

2. Sovereign Infrastructure as a Battlespace

The National Security Strategy 2025 signals an explicit doctrinal evolution in the treatment of national infrastructure. Where earlier frameworks tended to regard critical infrastructure as an enabler of economic stability, NSS 2025 formally designates it as a strategic domain, one that is not only vulnerable to adversarial disruption but is now central to the conduct of modern conflict [1]. In doing so, the Strategy reflects both the operational logic of peer adversaries and the lived reality of sub-threshold hostility targeting the United Kingdom.

Undersea Cables

Over 99 percent of the UK's digital data traffic, including financial services, communications, logistics, and defence coordination, transits through undersea cables that remain exposed to deliberate acts of sabotage, hostile probing, and clandestine mapping by adversarial actors.

Energy Pipelines

A substantial portion of the UK's gas supply is delivered through underwater pipeline networks, forming part of the arterial network of national functioning that remains vulnerable to interference.

Operation Atlantic Bastion

Led by the Royal Navy and integrated with allied surveillance capabilities through NATO Maritime Command and the Joint Expeditionary Force, providing persistent maritime presence to detect, track, and deter underwater threats.

This reclassification is neither symbolic nor incidental. The Strategy identifies undersea cables, energy pipelines, transportation nodes, digital networks, and data infrastructure as principal targets for adversaries employing hybrid tactics [1]. These systems are no longer considered passive assets to be protected in the event of escalation. They are now active theatres of contestation, already subject to reconnaissance, pressure and in some cases, hostile interference [3][4][5].

NSS 2025 responds with a threefold approach: forward defence, attribution readiness, and infrastructure denial. Operation Atlantic Bastion is the clearest manifestation of this shift. This forward posture is accompanied by revised Rules of Engagement that enable British warships to act with greater agility when confronting suspected sabotage operations. The significance of this policy change lies not in its assertiveness, but in its clarity. The United Kingdom is no longer signalling uncertainty in the face of sub-threshold threat. It is establishing expectations, both to allies and adversaries, that infrastructure interference will be treated as strategic hostility [1].

Infrastructure Defense Strategy

This approach mirrors adversary doctrine. Russia's hybrid warfare model places considerable emphasis on targeting dual-use infrastructure, often in ways that maintain plausible deniability while achieving disproportionate strategic disruption [3]. Chinese systems confrontation theory similarly identifies chokepoints in data and energy flows as levers of geopolitical pressure [4]. Iran has demonstrated an ability to blend asymmetric sabotage with criminal networks to undermine regional infrastructure and conceal attribution [5]. NSS 2025 reflects an institutional understanding that these doctrines are operational, coordinated, and designed to weaken national will without the need for conventional escalation.

In response, the Strategy also expands the scope of homeland security to include the defence of infrastructure against both physical and digital intrusion. This includes investment in cyber defences for energy distribution systems, increased counter-surveillance in port and logistics hubs, and a renewed emphasis on resilience within the supply chain architecture [1]. These measures are not framed as insurance. They are presented as elements of active denial, intended to raise the cost of disruption and frustrate the adversary's capacity to act with impunity.

Importantly, the Strategy also recognises the interdependence between civil infrastructure and military capability. Satellite uplinks, cloud compute, high-voltage substations, and logistics corridors now underpin the operational tempo of modern forces. Adversaries are well aware of this convergence and have tailored their targeting models accordingly. In this context, civil-military fusion is not a peacetime coordination exercise but a warfighting necessity [1].

Beyond the technical measures, NSS 2025 also seeks to anchor infrastructure defence within a wider campaign of public legitimacy. It does so by reasserting the notion that security is a shared burden. The Strategy introduces resilience exercises, awareness campaigns, and infrastructure audits not as bureaucratic functions, but as national endeavours. The intent is to cultivate a societal posture that understands, supports, and actively participates in the defence of the national commons [1].

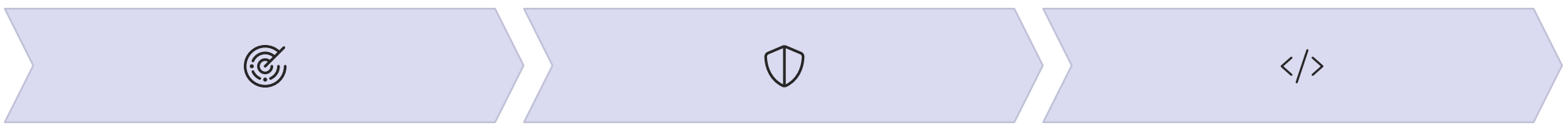
The cumulative effect of this doctrine is a return to first principles: that national strength rests not only on capabilities, but on control. Infrastructure, once assumed to be protected by distance, convention, or legal status, is now seen as a terrain of contest. The adversary recognises this. The United Kingdom must do the same. In treating infrastructure as a battlespace, NSS 2025 does not declare confrontation. It acknowledges that confrontation is already under way and asserts that sovereignty, in the 21st century, begins with retention of control over the systems that keep the nation functioning under pressure.

References

1. National Security Strategy 2025, CP 1338, HM Government, 24 June 2025
2. Reuters, "UK to broaden security focus, set 5% defence spending target", 23 June 2025
3. MOD SDR 2025, Section 3.4, "Hybrid and Reflexive Adversary Threats", 2 June 2025
4. Financial Times, "UK identifies China's systems confrontation doctrine", 24 June 2025
5. AP News, "Iran's asymmetric playbook targeting the UK", 23 June 2025

3. CyberEM Command and the AI-Defined Force

Among the most consequential developments in the National Security Strategy 2025 is the formal introduction of a new organisational and operational layer within the British Armed Forces: the Cyber Electromagnetic (CyberEM) Command. It is accompanied by an unequivocal ambition to deliver a tenfold increase in the Army's lethality by 2035, driven not only by traditional platforms but by the integration of artificial intelligence, autonomous systems, and precision-guided software-defined targeting. Taken together, these measures reflect the UK's recognition that future deterrence and defence will be determined as much by logic-layer dominance as by firepower.



Spectrum Superiority

CyberEM Command is structured to provide persistent decision advantage in environments where bandwidth is contested, latency is decisive, and attribution is deliberately obscured.

Cyber Resilience

Positioned as a core component of joint force design, cutting across conventional domains and assuming equal footing in operational planning.

AI-Supported Targeting

Creation of a Digital Targeting Web, a networked environment in which sensors, shooters and command elements are fused through real-time data exchange.

This transformation is doctrinal as well as technical. CyberEM Command is not framed as a specialist adjunct to existing capability. Its remit includes spectrum superiority, electromagnetic warfare, cyber resilience, offensive cyber operations, and AI-supported targeting architecture. Crucially, it is structured to provide persistent decision advantage in environments where bandwidth is contested, latency is decisive, and attribution is deliberately obscured [1].

This reflects a shift from the traditional view of cyber as a supporting capability to a more contemporary understanding of it as a domain of warfare in its own right. The decision to unify cyber and electromagnetic operations under a single command structure acknowledges the evolving nature of adversarial threat. Russian electronic warfare doctrine, for example, emphasises the coordinated disruption of command-and-control systems, satellite links, and positioning, navigation and timing services, often in tandem with kinetic operations [2]. China's systems suppression strategies prioritise digital infrastructure, space-based assets and electromagnetic dominance in the early phases of confrontation [3]. Iran has repeatedly used cyber operations to delay attribution and impose strategic cost without conventional escalation [4]. NSS 2025 responds to this convergence not by mimicking their tactics, but by reorganising British capability around the same strategic centre of gravity: control of the information and decision environment.

The stated aim of increasing the Army's lethality by a factor of ten by 2035 is not rhetorical. It is grounded in an analysis of force effectiveness under modern conditions. The Strategy identifies five vectors of transformation: long-range precision fires, autonomous systems, enhanced battlefield awareness, AI-assisted targeting and a digitally fused command structure [1]. These are not presented as future aspirations, but as current imperatives, informed by the ongoing adaptation of Ukrainian and Russian forces on the battlefield and by the broader shift in warfare from platform-centric to network-centric models.

Force Transformation and Investment

To deliver this capability, the government has committed to major capital investment across the defence-industrial ecosystem. This includes the procurement of up to 7,000 domestically built long-range weapons, the establishment of new munitions and energetics factories, and the expansion of sovereign compute and AI infrastructure [5]. From 2026, the Ministry of Defence will allocate at least 10 percent of its equipment procurement budget to novel technologies, creating a sustained innovation pathway aligned with operational demand [1].

7,000

Long-Range Weapons

Domestically built precision weapons to be procured as part of the force transformation

10%

Innovation Budget

Minimum allocation of equipment procurement budget dedicated to novel technologies from 2026

10x

Lethality Increase

Targeted improvement in Army's combat effectiveness by 2035 through AI and autonomous systems

The implications of this posture are far-reaching. For the first time in formal doctrine, software is treated as a decisive component of force. The Strategy commits to the creation of a Digital Targeting Web, a networked environment in which sensors, shooters and command elements are fused through real-time data exchange and AI-enabled decision support [1]. This system is designed not only to accelerate targeting cycles, but to enable lawful and auditable execution under degraded conditions. In effect, it seeks to preserve sovereign control of targeting logic even when communications are contested or denied.

This initiative speaks directly to the operational methods of peer adversaries. It is now broadly accepted that both Russia and China have sought to accelerate the pace of conflict through automation, decision interference, and spectrum denial [3]. In such an environment, the capacity to maintain internal coherence, to hold a consistent and lawful targeting process while under digital attack, becomes not just a matter of tactical advantage, but of strategic legitimacy.

The introduction of CyberEM Command is also a structural acknowledgement that adversarial activity will often begin in the information and electromagnetic domains, rather than transition into them. The UK's posture, therefore, is shifting to one of pre-emptive orientation, not to strike first, but to see clearly, respond coherently, and impose friction on adversary manoeuvre before thresholds are crossed. In this sense, cyber and AI capability are no longer viewed as technical augmentations. They are treated as foundational to deterrence, a position long adopted by adversaries but now formally embraced within British doctrine.

Alongside capability development, the Strategy also recognises the need for institutional agility. CyberEM operations demand flatter command structures, mission-type orders, and high levels of cross-service interoperability. They also require the integration of non-traditional actors, including academia, private sector partners and classified innovation units, into defence planning cycles. NSS 2025 supports this shift by expanding access to private capital, creating incentives for dual-use innovation, and introducing reforms to procurement law that favour speed, flexibility, and iterative adaptation [1][5].

At the strategic level, these reforms carry implications for alliance planning. The Strategy reaffirms the centrality of NATO but asserts a sovereign approach to capability generation. The United Kingdom's contributions to AUKUS, the Global Combat Air Programme, and Five Eyes cyber cooperation are intended to complement NATO force structure, not replace it. However, the clear message is that the UK intends to retain freedom of manoeuvre in capability development, particularly in the cyber and AI-enabled domains. This posture reflects both national ambition and an understanding of how peer adversaries approach interoperability, selectively, strategically and always in support of sovereign decision-making.

In sum, National Security Strategy 2025 treats cyber and AI capability not as future dilemmas, but as present conditions. The introduction of CyberEM Command and the redesign of force around digital lethality reflect a mature understanding of how adversaries operate, how decision dominance is contested, and how warfare is evolving in practice. It is a posture rooted in realism, but designed for initiative. In an environment defined by tempo, ambiguity, and disruption, the ability to command coherence under pressure will determine not only tactical outcomes, but national sovereignty itself.

References

1. National Security Strategy 2025, CP 1338, HM Government, 24 June 2025.
2. UK MOD, Strategic Defence Review 2025, Section 3.4: Electromagnetic and C2 Threats, 2 June 2025.
3. Financial Times, "UK identifies China's digital and space strategy as principal doctrinal challenge", 24 June 2025.
4. AP News, "Iran cyber attacks UK critical infrastructure amid wider alignment with Russia", 23 June 2025.
5. The Guardian, "Defence review plans will make army '10 times more lethal', says John Healey – as it happened", 2 June 2025.

4. Calibrating Doctrine – NSS 2025 and the Adversarial Grey Zone Playbook

The National Security Strategy 2025 marks a significant maturation in British strategic thinking, not only in the capabilities it sets forth, but in the adversary it recognises. For the first time in formal state doctrine, the United Kingdom explicitly acknowledges that it is operating against peer competitors who have developed and institutionalised their own playbooks for coercion below the threshold of war. These are not abstract threats. They are active frameworks, codified in foreign doctrine, tested in the field, and now visibly aligned across theatres.

NSS 2025 recognises this convergence. It does so not by declaring equivalence between adversaries, but by studying the logic that underpins their operations and aligning British posture accordingly. This section provides a doctrinal calibration, comparing the assumptions, objectives, and tools of the UK's principal adversaries with the structural shifts set out in the Strategy. It affirms that Britain is not only adapting to an uncertain environment. It is responding directly to adversaries who have already moved, with speed, coherence, and intent into the Grey Zone.

Russia: Reflexive Control

Manipulates the information environment to induce adversaries to act against their own interests through orchestration of ambiguity, fragmentation, and delay, supported by cyber attacks, sabotage, and selective escalation below attribution thresholds [3].

China: Systems Confrontation

Emphasizes targeting of command networks, economic dependencies, narrative space, and digital ecosystems in a coordinated campaign designed to delay or disable an adversary's capacity to respond [4].

Iran: Asymmetric Disruption

Blends statecraft with paramilitary, criminal, and proxy elements to generate persistent disruptive effect across multiple domains, often deniable and calibrated to impose strategic cost without direct attribution [5].

Russia: Reflexive Control and Strategic Pressure

The Russian Federation has long operated on the principle that perception is the battlefield. Through its doctrine of reflexive control, Russian military thinkers have sought to manipulate the information environment in order to induce adversaries to act against their own interests. This approach extends beyond propaganda or disinformation. It is characterised by the deliberate orchestration of ambiguity, fragmentation, and delay, often supported by cyber attacks, sabotage, and selective escalation below attribution thresholds [3].

NSS 2025 responds to this by placing national decision-making coherence at the centre of its defence posture. The introduction of a Digital Targeting Web, the investment in sovereign AI infrastructure, and the emphasis on lawful targeting even under degraded conditions are direct counters to the Russian model of tempo manipulation [1]. Moreover, the Strategy's prioritisation of domestic readiness, including undersea cable defence, resilience drills, and public awareness campaigns, is designed to deny the adversary the opportunity to induce paralysis at the strategic level [1][3].

China: Systems Confrontation and Information Dominance

China's approach is rooted in a long-view understanding of strategic influence. Its doctrine of systems confrontation emphasises the targeting of command networks, economic dependencies, narrative space, and digital ecosystems in a coordinated campaign designed to delay or disable an adversary's capacity to respond [4]. Within this framework, cyber operations, information warfare, trade leverage, and even legal interpretation are employed as instruments of systemic pressure.

NSS 2025 demonstrates a conscious understanding of this doctrine. It embeds economic security directly into its national security model, expanding the remit of deterrence to include supply chains, intellectual property, digital standards and regulatory sovereignty [1]. The Strategy's emphasis on creating asymmetric technological advantage, particularly in AI, semiconductors, and quantum computing, reflects a deliberate effort to preclude dependency and maintain initiative in contested domains [1][4].

The UK's recommitment to AUKUS and its strategic technology partnerships with Japan and the United States are also shaped by this context. These are not mere capability programmes. They represent efforts to build a trusted sovereign ecosystem that can resist fragmentation, a direct counterweight to Beijing's vertical integration of diplomacy, trade, and defence under the mantle of coercive interoperability [4].

Adversarial Strategies and UK Response

Iran: Proxy Integration and Asymmetric Disruption

Iran's playbook is distinct in form, but no less strategic in ambition. It blends statecraft with paramilitary, criminal, and proxy elements to generate persistent disruptive effect across multiple domains. From cyber attacks on UK institutions to surveillance of dissident communities in London, Iran's activities are often deniable, often persistent, and always calibrated to impose strategic cost without direct attribution [5].

The NSS addresses this threat explicitly. It includes Iran alongside Russia in the enhanced tier of the Foreign Influence Registration Scheme, mandates visa denial for individuals seeking to incite domestic division, and outlines sanctions against Iranian-linked criminal networks [1]. It further empowers Counter Terrorism Policing to investigate state threat offences and commits to legislation modelled on counter-terrorism powers to counter malign foreign activity [1].

What is notable, however, is the integration of these measures into a broader doctrine. The Strategy does not treat Iranian activity as isolated disruption. It is positioned within the same doctrinal logic as Russia and China, that of protracted, layered, sub-threshold confrontation. As such, the UK's response is not limited to defensive posture, but extends to pre-emptive denial, diplomatic hardening, and societal resilience.

Adversarial Alignment: Strategic Collusion Across the Grey Zone

The most strategically important development in NSS 2025 is its recognition that adversaries are no longer acting in isolation. The Strategy draws attention to the growing synchronisation between states such as Russia, China, Iran, and North Korea, a pattern that extends beyond opportunism and increasingly reflects shared intent. North Korean deployments in support of Russian operations in Ukraine, Iranian drone supply chains feeding into the same theatre, and Chinese efforts to sustain the Russian defence-industrial base are cited not as isolated transactions, but as indicators of strategic parallelism [1][3][4][5].

This is not formal alliance in the traditional sense, but it reflects a convergence of method, timing, and tolerances. These actors have developed a common understanding of how to operate within and occasionally just outside the threshold of escalation, enabling them to apply coordinated pressure without triggering a unified Western response. NSS 2025 engages with this dynamic by framing British strategy as a sustained campaign rather than a series of reactions. That campaign is designed to resist not only individual threats, but the accumulated effects of long-term adversarial alignment.

This is reflected in the design of the Strategy itself. Investments in critical infrastructure resilience, the deepening of sovereign technological capability, and the integration of law enforcement, diplomacy, and military planning are all shaped by the understanding that modern coercion does not arrive all at once. It builds, it layers, and it operates across seams. The British response therefore privileges tempo, internal coherence, and sovereign control across domains.

Where adversaries have sought to exploit ambiguity, the UK positions itself around clarity of doctrine and lawful adaptability. Where pressure is applied through infrastructure and narrative, the Strategy strengthens societal resilience and narrative integrity. And where adversarial systems rely on deniability and fragmentation, NSS 2025 seeks to impose cost through persistent campaigning and systemic denial.

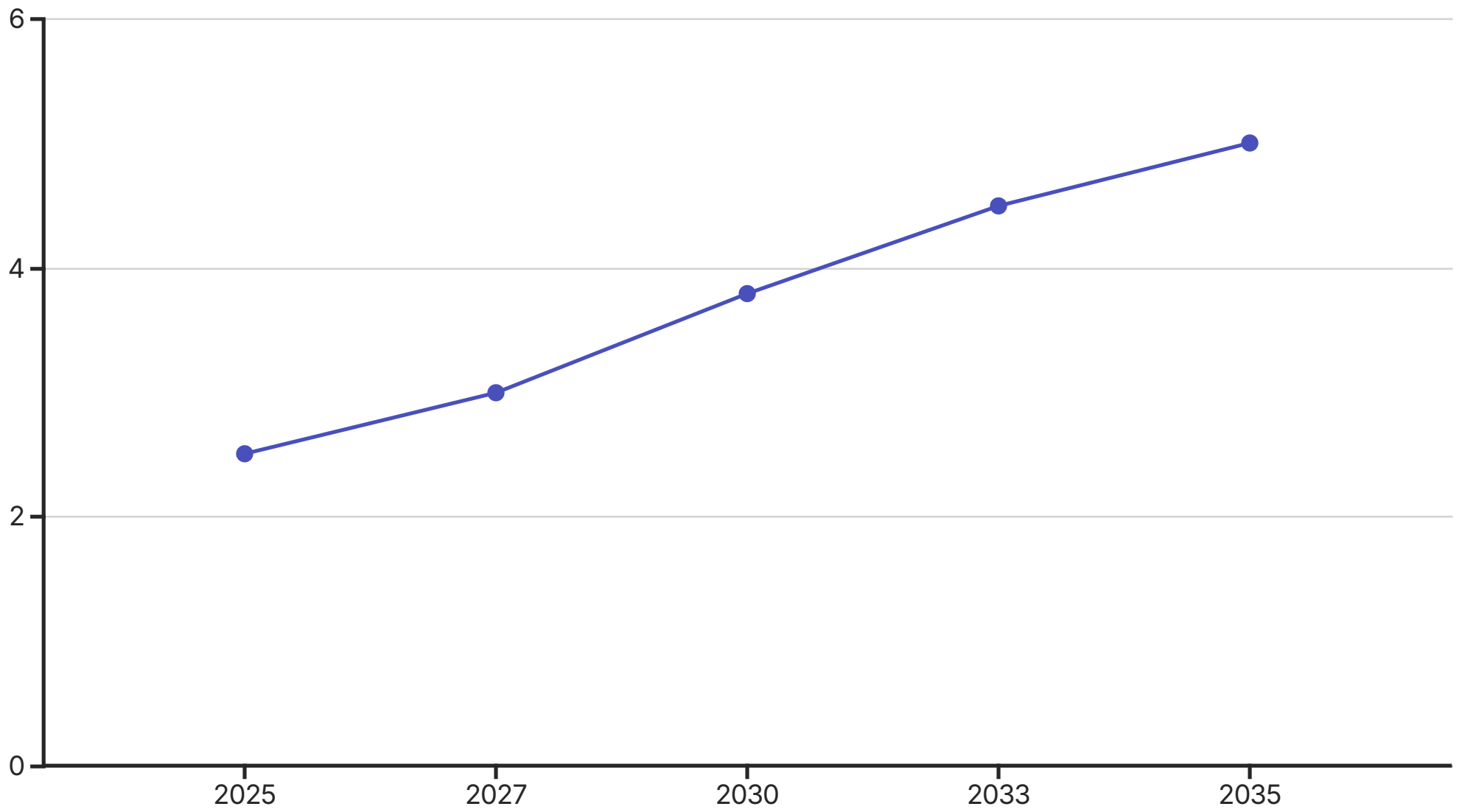
In that sense, the document is not merely reactive. It reflects an institution that has studied its challengers closely, understood the logic of their methods, and begun to reorganise national power around the kinds of friction and velocity that modern deterrence requires.

References

1. National Security Strategy 2025, CP 1338, HM Government, 24 June 2025
2. Reuters, "UK to broaden security focus, set 5% defence spending target", 23 June 2025
3. MOD SDR 2025, Section 3.4, "Hybrid and Reflexive Adversary Threats", 2 June 2025
4. Financial Times, "UK identifies China's systems confrontation doctrine", 24 June 2025
5. AP News, "Iran's asymmetric playbook targeting the UK", 23 June 2025

5. National Security as Economic Doctrine

A defining characteristic of National Security Strategy 2025 is its integration of economic security into the centre of the UK's defence posture. This is not simply an acknowledgement that prosperity underpins national strength. It is a doctrinal recognition that economic coherence, industrial depth, and technological sovereignty are now preconditions for strategic resilience.



The government's commitment to raise national security spending to 5 percent of GDP by 2035 reflects this shift in full. Framed not as a temporary uplift but as a generational realignment, the increase is intended to anchor defence policy within the broader mission of national renewal. The Strategy connects this investment directly to the domestic industrial base, to employment and regional regeneration, and to the state's ability to shape strategic outcomes at home and abroad [1][2].

This marks a deliberate departure from earlier models of compartmentalised policymaking, in which defence, economic policy, and technological development were often treated as parallel efforts. Instead, NSS 2025 aligns these elements within a unified strategic construct. Defence spending is no longer treated solely as insurance against external threat, but as an engine of economic transformation, one that can renew capacity in key sectors, drive sovereign innovation and create a more resilient national foundation in the face of persistent competition [1].

The Strategy identifies multiple domains in which this economic-security fusion is already under way. AUKUS and the Global Combat Air Programme are presented not only as defence collaborations, but as platforms for industrial policy, export leverage, and technological advantage. Domestic production of long-range munitions, the construction of energetics factories, and investment in shipbuilding capacity are aligned with both sovereign deterrence and local regeneration. This is supported by reforms to procurement law, including the ability to prioritise speed, domestic value, and industrial resilience in acquisition decisions [1][2].

Central to this approach is the emphasis on sovereign capability. The Strategy outlines an active role for the state in identifying and nurturing sectors where the UK must retain decisive national control. This includes high-performance computing, next-generation telecommunications, semiconductor design, and space-based assets, all of which are treated as strategic enablers rather than commercial ventures alone. Where market forces are insufficient to guarantee security, the government signals its willingness to intervene, including through public capital, regulatory instruments and, where necessary, legislative protection [1].

Economic Security and Strategic Contestation

This reorientation also acknowledges the adversarial context. China's ability to integrate trade, industrial policy, and statecraft into a coherent projection of national power has placed economic dependency at the heart of strategic contestation. Russia's adaptation of illicit finance and sanctions circumvention as tools of grey zone warfare has eroded assumptions about the separability of conflict and commerce. Iran's use of industrial and logistics networks to mask proxy activity has demonstrated how economic flows can be manipulated to achieve military effect [3][4][5].

Strategic Sectors

- High-performance computing
- Next-generation telecommunications
- Semiconductor design
- Space-based assets
- Clean energy
- Rare earth materials

Investment Initiatives

- AI growth zones
- Sovereign compute capacity
- £2.5 billion for nuclear small modular reactors
- Domestic munitions production
- Energetics factories

Policy Instruments

- Public capital investment
- Regulatory frameworks
- Procurement law reforms
- Legislative protection
- Supply chain security measures

NSS 2025 does not imitate these methods, but it responds to them. It does so by treating national economic architecture not only as an object of defence, but as a strategic instrument in its own right. The Strategy commits to protecting critical supply chains, increasing access to sovereign materials, and reducing exposure to hostile leverage, particularly in sectors such as clean energy, rare earths, digital infrastructure and industrial compute [1].

The same logic is extended to innovation. The government's support for AI growth zones, the expansion of sovereign compute capacity, and the creation of a £2.5 billion investment pipeline into nuclear small modular reactors are all framed as national security initiatives. These are not isolated industrial strategies, but elements of a broader campaign to ensure that the UK can shape, rather than absorb, the technological trajectory of contested domains [1][2].

Importantly, this framing also carries implications for alliance behaviour. Sovereign economic capability is not treated as a retreat from cooperation, but as a prerequisite for credible participation in it. The Strategy highlights that greater burden-sharing within NATO, deeper interoperability with the United States, and sustained European engagement will all require the UK to generate its own resilience, not only in defence outputs, but in the economic foundations upon which operational credibility depends [1][2].

In this light, National Security Strategy 2025 offers not just a new vision for defence policy, but a reframing of national power itself. It suggests that in a world where coercion is cumulative and confrontation is layered, the strength of a nation lies in its ability to align resources, institutions, and industries around a shared sense of strategic purpose. Sovereignty, in this model, is not defensive or isolationist. It is the capacity to act with consistency, to shape one's options, and to carry weight in a system increasingly defined by volatility and selective interdependence.

This is the economic doctrine embedded within NSS 2025, one that treats national resilience as a function of cohesion, and national influence as an outcome of control.

References

1. National Security Strategy 2025, CP 1338, HM Government, 24 June 2025
2. Reuters, "UK to broaden security focus, set 5% defence spending target", 23 June 2025
3. MOD SDR 2025, Section 3.4, "Hybrid and Reflexive Adversary Threats", 2 June 2025
4. Financial Times, "UK identifies China's systems confrontation doctrine", 24 June 2025
5. AP News, "Iran's asymmetric playbook targeting the UK", 23 June 2025

6. Conclusion and Strategic Recommendations

National Security Strategy 2025 represents more than an updated policy statement. It signals the conscious reconfiguration of British statecraft to match the pressures of a new strategic era. The document accepts that the operating environment has changed, not through declaration or invasion, but through a gradual recalibration of power, risk, and legitimacy by capable adversaries who no longer wait for overt conflict to pursue their aims.

The Strategy moves with deliberation. It recognises that the UK must now conduct itself in a world shaped by cumulative pressure rather than discrete episodes. In this environment, the tools of statehood, from infrastructure and investment policy to information systems and societal cohesion, are subject to persistent contest. The Strategy responds by binding these instruments together within a single campaigning posture: forward-leaning, adaptive, and legally anchored.

Economic policy is treated not as adjacent to defence, but as integral to national security. So too are digital infrastructure, civil preparedness, and technological sovereignty. The ambition is not to centralise control, but to recover coherence. From undersea cables to cloud compute, from AI-enabled targeting to industrial regeneration, the Strategy builds the case for a sovereign foundation capable of withstanding both overt challenge and ambient disruption.

Crucially, this is not a declaration of transformation already achieved. It is the start of a disciplined process, one that will require consistent ministerial leadership, institutional tempo, and national patience. Britain is not returning to a static defensive posture. It is beginning to campaign, structurally, across all domains in which adversaries now operate.

Strategic Recommendations

Establish a Unified Campaigning Doctrine for Sub-Threshold Operations

A formal, whole-of-government doctrine should be developed to embed the principles of campaigning across defence, diplomacy, law enforcement, and economic regulation. This doctrine must shape how the UK prepares for, absorbs, and responds to prolonged strategic friction, rather than treating such activity as a temporary anomaly.

Protect Decision Infrastructure as a Strategic Asset

The systems that underpin lawful command, AI logic, and targeting integrity must be prioritised as critical infrastructure in their own right. Protection, redundancy, and sovereign legal authority must extend across digital, electromagnetic, and procedural layers. The ability to operate under pressure will depend on confidence in these systems above all.

Bring the National Security and Investment Act into Active Use

The National Security and Investment Act 2021 offers a legal architecture fit for the current environment. To date, however, it has functioned more as a latent safeguard than a proactive tool. It should now be deployed with clear strategic direction, ensuring that foreign investment, IP transfers, and corporate control in sensitive sectors are scrutinised as part of an active security doctrine. The legislation should be seen not as a barrier to openness, but as a means of maintaining strategic freedom of action in key domains.

Embed Infrastructure Defence into Operational Command

Physical and digital infrastructure must be integrated into national deterrence planning. This includes subsea monitoring, port and substation resilience, energy distribution security, and narrative continuity during periods of denial or disruption. Responsibilities should be assigned across departments, with standing authorities to act within pre-agreed thresholds.

Align International Partnerships with a Clearly Articulated Sovereign Base

The UK's contributions to collective security arrangements should be underpinned by sovereign capabilities in areas where reliance introduces friction or constraint. The Strategy rightly recommits to NATO and AUKUS, but future participation in joint endeavours must be built on a foundation of credible, independent capability, particularly in AI ethics, data standards and supply chain control.

Britain has not chosen the conditions under which it now operates. But it has chosen to respond with realism, coherence and resolve. The adversary campaigns through ambiguity. The Strategy makes clear that the United Kingdom intends to respond with clarity, not as provocation, but as posture. From this point forward, national security will be measured by more than capability. It will be measured by whether that capability can be brought to bear, in time, under pressure and with purpose.

References

1. National Security Strategy 2025, CP 1338, HM Government, 24 June 2025
2. Reuters, "UK to broaden security focus, set 5% defence spending target", 23 June 2025
3. MOD SDR 2025, Section 3.4, "Hybrid and Reflexive Adversary Threats", 2 June 2025
4. Financial Times, "UK identifies China's systems confrontation doctrine", 24 June 2025
5. AP News, "Iran's asymmetric playbook targeting the UK", 23 June 2025