DEFENCE HOLDINGS

DEFENCE HOLDINGS PLC

The Hidden Front Line
Securing UK Sovereignty in the Digital Age

This whitepaper examines the shifting meaning of sovereignty in the digital age, where cloud platforms, algorithms, and AI are as decisive as ships and aircraft once were. It explores the UK's deepening partnerships with hyperscalers and US defence primes, alongside the vulnerabilities these dependencies create. It argues that true sovereignty requires balance, allied cooperation on one hand, and deliberate investment in sovereign capability on the other.

defenceplc.com

White Paper | Published 24 September 2025

72 Charlotte Street, London, England, W1T 4QQ.
Company number 12187837.

Executive Summary

— To secure resilience, the UK requires sovereign capabilities.

> In the last century, sovereignty could be photographed. It was visible in the hulls of warships, the roar of fast jets, the silos of nuclear missiles. A sovereign nation was one that could design, manufacture, and command its own arsenal.

In this century, sovereignty is harder to see but no less decisive. It lies in code, in cloud platforms, in algorithms. It resides in the invisible infrastructure that underpins defence, resilience, and trust.

Over the past week, the UK has taken significant steps in this arena. The UK–US Tech Prosperity Agreement was signed, formalising deeper bilateral cooperation on advanced technologies. Expanded partnerships with hyperscale providers, AWS, Microsoft, Google, and Oracle, were confirmed, reinforcing their role at the core of UK cyber and defence systems. Palantir's ongoing contracts in defence analytics were renewed, embedding powerful but foreign-owned platforms into critical UK workflows. Alongside these developments, Defence Holdings has increasingly been recognised as one of the emerging assets in the UK's wider push for resilience.

Each of these partnerships brings immense capability. They are indispensable. Yet they raise a central question: how can the UK ensure sovereignty means more than access to allied technologies?

The recent cyberattack on Heathrow offered a stark reminder. A disruption to civilian infrastructure rippled across national life. It was not a missile strike, but its impact was strategic. Sovereignty in the digital era is not abstract. It is tested every day.

This whitepaper explores that test. It examines the role of Big Tech in UK defence and cyber security, analyses vulnerabilities and adversarial playbooks, and assesses the UK's policy and industrial landscape. It concludes with closing reflections: hyperscale partners are essential, but sovereignty requires ownership, direction, and freedom of action.

Sovereignty

— Sovereignty in the Digital Battlespace

For much of the last century, sovereignty was defined by physical assets: ships, aircraft, tanks, and missiles. These were capabilities the state could own and operate directly. Today, the decisive frontier is digital.

Infrastructure has dematerialised. Fibre-optic cables, server farms, and cloud platforms are as strategic as steel and oil once were. Information is no longer just a tool of policy; it is the terrain itself.

Conflict has become ambient. Cyberattacks, disinformation campaigns, and hybrid operations blur the line between peace and war. The Heathrow hack was not an act of open conflict, but it demonstrated how national confidence and operational readiness can be undermined without a shot being fired.

Control has migrated because the critical systems of the digital age, cloud platforms, data pipelines, and AI models, are developed and operated by the private sector. Most of the providers with the scale to deliver them are headquartered outside the UK. Their incentives are commercial and global, which does not always align neatly with the requirements of national sovereignty.

These companies bring extraordinary capability and are indispensable to UK defence. The issue is not the value of partnership, but the absence of sovereign safeguards. Without them, reliance can harden into dependency, reducing the UK's room for manoeuvre in times of crisis.

Sovereignty

— Big Tech as Strategic Partners

Over the past decade, global technology companies have become embedded in the core of UK defence and security.

This is not a future prospect; it is already a fact of national life. The Ministry of Defence, the intelligence agencies, and wider government now rely on systems and platforms provided by a small number of firms whose scale cannot be replicated domestically.

The **hyperscale providers,** AWS, Microsoft, Google, and Oracle, supply the backbone of the UK's cloud, AI, and cyber infrastructure. They provide the resilience and processing capacity required to manage modern defence workloads, from secure communications and logistics to the storage of vast intelligence datasets. Without them, much of the UK's digital infrastructure would simply not function at the scale required.

Palantir occupies a different but equally central position. Its advanced analytics platforms are used across defence and national security missions. From logistics in Ukraine to data fusion in Whitehall, Palantir has demonstrated the ability to integrate multiple streams of information and render them usable in near real time. For UK decision-makers, the attraction is obvious: capability delivered now, with proven track record.

Anduril represents another strand of this ecosystem. Known for autonomous systems and situational awareness platforms, it has built a reputation for rapid innovation cycles, deliberately positioning itself as an alternative to slower-moving defence primes. Its technology is increasingly visible in allied procurement pipelines, including the UK.

And above these company-specific relationships sits the UK–US Tech Prosperity Agreement, signed to enshrine closer cooperation on advanced technologies. It formalises what has already been reality: the UK's sovereign capability is deeply intertwined with that of its allies, and particularly with US technology ecosystems.

None of this is optional. These partnerships are essential. The UK gains access to scale, resilience, and innovation that no domestic ecosystem could provide alone. In the short term, this strengthens capability and reduces risk. But in the long term, it raises serious questions.

The first is **jurisdictional risk**. Hyperscalers are governed by the laws of their home states. For US-based companies, this includes the CLOUD Act, which can compel disclosure of data stored on their systems, regardless of where that data physically resides. For the UK, this creates the possibility that critical workloads could be subject to foreign legal obligations, intersecting with sovereignty in ways that are complex and not always transparent.

The second is **narrative risk**. Palantir and Anduril often position themselves as champions of sovereignty within UK debates. Their marketing frames their platforms as guarantors of independence. Yet as US businesses, their ultimate alignment lies with Washington, not Westminster. This is not a question of intent or goodwill. It is a structural fact. When sovereignty is defined by ownership and freedom of action, foreign-owned platforms cannot fully deliver it.

The third is **industrial risk**. The UK's domestic industry is innovative and capable. From AI firms such as Faculty and Mind Foundry to cyber specialists like Darktrace and Roke Manor, there is no shortage of sovereign talent and intellectual property. Yet these firms often remain under-leveraged, unable to scale within procurement frameworks that default to foreign primes. Without deliberate intervention, the gap will widen: the UK will continue to produce ideas, while the platforms that operationalise them are controlled abroad.

The challenge, therefore, is not whether to work with hyperscalers and primes. The UK must, and it will. The challenge is how to integrate them within sovereign frameworks that ensure dependency does not harden into exclusivity. That means contracts structured with safeguards, architectures that allow sovereign override, and procurement that deliberately nurtures British innovation alongside global partnerships.

> True sovereignty lies in the ability to act independently when required. It is not about rejecting allies or retreating from partnerships, but about retaining ownership of intellectual property, direction of development, and freedom of action in times of crisis. Allied partnerships strengthen capability. Sovereign capability secures independence. The UK requires both, and must now decide how to balance them.

Sovereignty

— Case Studies in Dependency

Heathrow Cyberattack (2025)

At 6.17am on a July morning, departures at Heathrow slowed to a crawl. Screens froze. Queues lengthened. By mid-morning, news outlets were running headlines about “system failures” and stranded passengers. In truth, Heathrow had been hacked. Flights were delayed, logistics chains were interrupted, and public confidence faltered. The breach was not catastrophic, yet it revealed the vulnerability of critical civilian infrastructure. Heathrow was targeted because it is symbolic. The disruption was not about grounded aircraft alone, but about shaking confidence in national resilience. The attack underscored three truths. Civilian infrastructure is a frontline. The battle space now includes transport hubs, utilities, hospitals, and energy grids. Hybrid disruption is cumulative: even limited incidents, when repeated, exhaust security resources and sow public doubt. And sovereign control is limited. The systems underpinning Heathrow, from cloud platforms to vendor networks, are not fully UK-owned. Sovereignty without control of the digital stack is fragile.

Palantir in UK Defence

Palantir provides advanced analytics platforms that support UK defence, security, and intelligence operations. Its capabilities are powerful. But the question is not whether Palantir strengthens the UK, it clearly does. The question is what sovereignty means when core decision systems are provided by foreign-owned platforms.

Who owns the datasets and models trained within them? Can the UK adapt or redirect the platform without external approval? When Palantir presents itself as the champion of UK sovereignty, is this rhetoric, or reality?

These questions do not diminish Palantir’s value. They sharpen the UK’s responsibility to define sovereignty for itself.

[continued....]

Sovereignty

Cloud Outages and Strategic Dependence

Hyperscale cloud platforms, AWS, Microsoft Azure, Google Cloud, Oracle Cloud, are indispensable to the UK's defence and security infrastructure. They provide resilience, capacity, and scale that no domestic ecosystem can replicate. But reliance carries risk. Outages can disrupt military and intelligence workloads. Providers are governed by US law, including frameworks such as the CLOUD Act, which can intersect with UK sovereignty. In a geopolitical crisis, platforms headquartered abroad may face conflicting obligations.

The lesson is that we need to embed hyperscalers within sovereign frameworks that guarantee UK direction and continuity, even under stress.

Sovereignty

— Adversarial Playbooks

If the UK's reliance on foreign platforms creates questions of sovereignty, adversaries have been quick to see the opportunity. Cyber and information operations are no longer experimental tools.

They are embedded in doctrine, funded at scale, and deployed systematically to destabilise open societies. Each adversary has its own playbook, but the logic is the same: exploit openness, amplify division, and erode confidence in institutions.

Russia: Hybrid Doctrine

Russia has been the most aggressive and consistent in integrating cyber and information warfare into its strategy. What began in Georgia in 2008 as crude website defacements and denial-of-service attacks has evolved into highly coordinated operations blending cyber intrusion, disinformation, and conventional force. In Crimea in 2014 and Ukraine in 2022, Russia did not simply send in troops. It prepared the ground with years of narrative warfare: questioning the legitimacy of Kyiv, spreading conspiracies about "fascists" and "neo-Nazis," and seeding doubt among Western publics about the cost of supporting Ukraine.

The GRU, Russia's military intelligence agency, has repeatedly orchestrated hacks of political organisations. In the United States, emails stolen from the Democratic National Committee were released at carefully chosen moments to shape the 2016 election narrative. In Europe, troll farms based in St Petersburg flooded social media with memes, falsehoods, and coordinated outrage. These were not side shows. They were part of Russia's wider hybrid doctrine: to exhaust, divide, and destabilise adversaries before, and during, physical confrontation.

China: The "Three Warfares"

China has taken a different route, but with equal determination. In 2003, the People's Liberation Army codified its "Three Warfares" doctrine: psychological, legal, and public opinion warfare. The doctrine is clear-eyed: shaping perceptions is as important as shaping battlefields.

Domestically, the strategy relies on censorship and control. Platforms such as WeChat and Weibo operate within a tightly managed information environment. Abroad, the approach is more subtle. TikTok, with its global reach, curates content flows that can shape perceptions indirectly. Chinese state media has invested heavily in Africa, Latin America, and Europe, presenting a narrative of China as a reliable partner and downplaying criticism of its policies.

In the South China Sea, China's approach has been both physical and informational. Land reclamation projects built artificial islands. Narrative reclamation framed those islands as historic entitlements, repeated until they became part of the discourse. This dual strategy, facts on the ground combined with stories in the air, demonstrates how sovereignty disputes are fought as much in perception as in geography.

Iran and North Korea: Asymmetric Actors

Smaller states have also found cyber to be a cost-effective asymmetric weapon. Iran has targeted critical infrastructure across the Gulf, seeking to disrupt energy supply and demonstrate reach. Its operations often combine physical sabotage with cyber intrusions, magnifying the psychological effect.

North Korea has pursued cyber for financial as well as strategic gain. Ransomware attacks and cryptocurrency thefts have generated vital revenue streams for a sanctioned regime. But Pyongyang has also used cyber tools to disrupt South Korean infrastructure and to signal capability against the West. These states cannot compete with NATO in conventional terms, but cyber allows them to punch far above their weight.

Proxy and Mercenary Groups

Perhaps the most troubling trend is the rise of semi-deniable cyber groups. These actors blur the line between state and non-state, providing hostile powers with plausible deniability. They are often recruited from criminal backgrounds or ideological fringes, operating for money, validation, or both.

Their tactics range from ransomware attacks to targeted sabotage. In Europe, Telegram channels linked to Russian networks have been used to recruit local operatives for small-scale but disruptive attacks: arson at supply depots, symbolic intimidation, even parcel bombs. Each act is minor in isolation. Together, they create a drumbeat of disruption that erodes confidence in security services and diverts resources. The Heathrow hack bears many hallmarks of this approach: disruptive, deniable, and cumulative. It was not designed to destroy infrastructure permanently, but to sow doubt and demonstrate vulnerability. Attribution is difficult, which is precisely the point.

The Implication

For the UK, the implication is clear. Sovereignty cannot be secured solely in the physical domain. It must extend to the digital and informational arenas where adversaries already operate as a matter of routine. Hybrid playbooks exploit dependencies, exploit open platforms, and exploit ambiguity. Without sovereign capability, the UK risks being permanently on the back foot, reacting to attacks rather than shaping the environment.

Sovereignty

— Comparative Sovereignty Strategies

In early 2024, a British court convicted three men of arson at a warehouse storing aid for Ukraine. On the surface, it appeared a criminal act with limited political significance.

Yet the details revealed a far darker pattern.The UK is not alone in facing questions of technological sovereignty. Every major power has had to confront the reality that control in the digital age looks very different from control in the industrial age. How each has responded reveals the range of strategic options available, and the limitations of the UK's current approach.

United States: Sovereignty by Default

For Washington, sovereignty is not a policy aspiration but a structural reality. The world's dominant hyperscale providers, AWS, Microsoft, Google, Oracle, are all American. So too are Palantir, Anduril, and a host of other firms that now provide the backbone of allied defence networks.
This means that when the Pentagon turns to Big Tech, it is turning to domestic companies. Programmes such as JADC2 (Joint All-Domain Command and Control) depend on the ability of these firms to provide data fusion, cloud processing, and AI-driven analytics at scale. The US may debate regulation or procurement preferences, but it does not question whether its core digital infrastructure is sovereign. It is. The challenge for Washington is not ownership but governance: how to balance the innovation of private firms with the oversight required for national security.

China: Sovereignty by Design

Beijing has taken the opposite path. Its doctrine is sovereignty by design, underpinned by the principle of military–civil fusion. Platforms such as Huawei, Baidu, Tencent, and ByteDance are either state-owned, state-controlled, or tightly aligned with government strategy. The boundary between commercial and strategic is blurred by design.

The Made in China 2025 programme explicitly prioritised control of semiconductors, AI, and next-generation communications as sovereign objectives. Where Western states see Big Tech as partners, China sees them as instruments of state power. Domestically, this provides security: Beijing can direct platforms at will. Internationally, it creates unease: Huawei's role in 5G networks, TikTok's reach into Western publics, and China's dominance of supply chains all raise questions about dependence.
For the UK, China's model is neither desirable nor replicable. It secures sovereignty at the cost of openness, embedding resilience by restricting freedom. But it demonstrates what can be achieved when a state sets sovereignty as a non-negotiable design principle.

European Union: Sovereignty by Regulation

Brussels has pursued sovereignty through regulation and coordination. The Digital Markets Act and Digital Services Act are designed to curb the dominance of US hyperscalers within the European market. At the same time, investment initiatives such as Gaia-X aim to create a federated European cloud, reducing reliance on external providers.

The EU does not possess the industrial base of the US or the state control of China, but it does have regulatory power. By setting standards, it seeks to shape markets in a way that protects European autonomy. This approach is defensive, often criticised for slowing innovation, but it reflects a deliberate calculation: better to constrain dependency than to ignore it.

United Kingdom: Between Models

The UK sits between these models. It benefits from agility, global connections, and close alliances with the US. Its openness has allowed rapid adoption of best-in-class technologies. But this openness has also created reliance. The UK cannot replicate US dominance. It will not follow China's model of state control. And it lacks the scale to wield regulation as Brussels does.

This leaves the UK in a unique position: open, allied, but dependent. Its sovereignty is partial, assured through alliances, but vulnerable in independence. The Heathrow hack, the Palantir contracts, the reliance on hyperscalers: each example illustrates the reality. The UK has capability, but not ownership. Access, but not independence.

The Strategic Choice

The lesson from these comparative strategies is not that one model should be copied wholesale. Each reflects specific political, economic, and cultural conditions. The lesson is that sovereignty must be deliberate. It cannot be assumed, and it will not emerge by accident.

For the UK, the choice is clear. Without a sovereign industrial base capable of anchoring partnerships, dependency will deepen. With one, the UK can remain open and allied while retaining the freedom to act on its own terms. Sovereignty does not require isolation. But it does require intent.

Sovereignty

— The UK Sovereign Tech Ecosystem

The UK does not lack ideas, talent, or innovation. What it lacks is scale. Beneath the surface of procurement frameworks dominated by foreign primes lies a vibrant ecosystem of sovereign firms, research institutions, and start-ups already delivering world-class technology. They are capable of anchoring British sovereignty, but too often they remain under-leveraged.

SMEs and Specialist Firms

Several UK companies have proven themselves at the cutting edge of AI, cyber, and information defence. Darktrace, spun out of Cambridge, pioneered AI-driven anomaly detection and now protects critical national infrastructure, government departments, and private firms alike. Its technology has shown that British-developed AI can compete globally, detecting and neutralising threats at machine speed.

Roke Manor Research, with a long pedigree in signals and cyber, continues to provide advanced mission analytics and operational cyber capability. Its engineers work on projects that intersect directly with national security, from electronic warfare to secure communications.

Oxford Dynamics, a lesser-known but strategically significant player, developed sovereign AI tools that supported elements of SDR25. Faculty and Mind Foundry, both with strong academic roots, build explainable AI platforms now being deployed across defence and intelligence. These firms are not hypotheticals. They are already delivering, already trusted, already sovereign.

Established Primes

The UK also retains established defence primes with deep technical expertise. QinetiQ, born from the Defence Evaluation and Research Agency, provides advanced robotics, mission systems, and cyber solutions. BAE Systems integrates cyber and electronic warfare capabilities into platforms ranging from submarines to combat aircraft. Nexor continues to be relied upon for secure information exchange at the highest assurance levels. Together, these primes demonstrate that the UK still has an industrial backbone. But they often deliver capability in partnership with US vendors, which dilutes the sovereign component.

The OSINT and Analytics Ecosystem

Another area of strength is open-source intelligence (OSINT). Start-ups such as OSINT Industries, and tools like Fivecast ONYX and ShadowDragon, are already used by law enforcement and counter-terrorism units. The Cabinet Office and techUK's INDEX platform is an attempt to standardise OSINT across government. This is an area where UK innovation could set a global benchmark. OSINT sits at the intersection of technology, analytics, and influence operations, precisely where sovereignty in the cognitive domain will be contested.

Sovereignty

Academia and Intellectual Capital

The UK's universities remain a sovereign jewel. Oxford's Machine Learning Group, Cambridge's Leverhulme Centre for the Future of Intelligence, and the London-based DeepMind continue to produce talent and research of world-class standard. The problem is not the quality of UK science. The problem is where its outputs end up. Too often, intellectual property generated in UK labs is absorbed into the R&D pipelines of hyperscalers. Sovereign IP becomes global IP, and national advantage dissipates.

The Integration Gap

When viewed in isolation, the pieces of the puzzle are impressive. But the system as a whole is fragmented. SMEs are too small to compete with the scale of US primes. Universities spin out start-ups that struggle to access capital. Large defence primes, while capable, often rely on foreign partners to deliver digital components.

What the UK lacks is a sovereign integrator, an entity with the mandate and resources to consolidate these capabilities into operational platforms. Without integration, innovation risks becoming export rather than advantage. With integration, the UK could build platforms that both anchor domestic resilience and enhance allied interoperability.

Defence Holdings' Role

This is where our own progress becomes relevant. We have positioned ourselves to act as part of that sovereign response. Our vision is to consolidate sovereign intellectual property into scalable platforms that underpin national security. In recent months, we have advanced product development in sovereign AI and formed partnerships across the defence ecosystem. Our role is not to compete with allies or hyperscalers, but to provide the sovereign anchor that ensures partnerships do not dilute independence.

The ecosystem exists. The innovation is proven. The talent is in place. The gap is integration and scale. If addressed, the UK could emerge not just as a consumer of foreign technology, but as a sovereign producer in its own right.

Closing Thoughts and Observations

The debate about sovereignty in technology is often framed in extremes: nations as either fully independent or dangerously dependent. The reality is more nuanced. The UK will always rely on alliances and partnerships. Hyperscale platforms and US defence primes are already woven into the fabric of national security. To deny this would be unrealistic.

But partnership is not sovereignty. Allies provide capability; they cannot confer independence. True sovereignty is the ability to act without permission, to decide on national terms, and to withstand pressure when interests diverge. It is not about rejecting partnerships, but ensuring they complement rather than compromise resilience.

Recent events have made this tension visible. The Heathrow cyberattack showed how civilian infrastructure can be targeted to undermine confidence. The UK–US Tech Prosperity Agreement confirmed the depth of allied interdependence. Palantir's renewed contracts illustrated both the value of foreign-owned platforms and the questions they raise about independence. Together, these episodes highlight a truth: sovereignty is not static. It is a balance to be managed continuously.

The UK's position is distinctive. It cannot replicate US industrial scale, follow China's model of state control, or wield the EU's regulatory heft. Its path must be its own: open, allied, but sovereign. That requires intent. Without it, dependency deepens. With it, the UK can work with allies while retaining the ability to act independently.

This perspective shapes our own work. Defence Holdings was conceived not to replace allies or hyperscalers, but to provide part of the sovereign anchor. Our vision — to build platforms that make sovereignty substance, not slogan — reflects the balance the UK itself must strike. In recent months we have advanced sovereign AI products and forged partnerships that embed British innovation in the defence ecosystem. We see ourselves as one of several emerging assets in the UK's wider push for resilience.

Sovereignty is not an endpoint or a prize held forever. It is a practice: an ongoing commitment to ownership, direction, and freedom of action. For the UK, the challenge is to embed that practice into the partnerships, policies, and platforms that will define the decades ahead.