Introduction

There is no doubt that we are living in a very unpredictable and uncertain geopolitical world. As Mark Carney, in his recent speech at Davos (1), made clear there is an ongoing 'rupture in the Rules Based International Order' which 'no longer functions as advertised' and shows complete disdain to transnational organisations, such as the UN, WTO and WHO, by the strongest powers. Effectively the big 3 powers believe that they can exempt themselves from such constraints, viz Russia's war on, and annexation of, large parts of Ukraine; the Chinese developing artificial islands in the South China Sea in order to claim ownership of international waters; and most recently the US seeking to annex Greenland, the semi-autonomous territory of Denmark, a NATO partner, along with the actions in Venezuela.

Similar views have also been expressed by Lawrence Wong, Prime Minister of Singapore who said in a recent interview(2), that 'we are in a transition to a post-American, multi-polar world and that it will be messy and unpredictable'. He observes that the 'old rules no longer apply but new ones have not yet been written, resulting in more turbulence ahead' and that countries cannot afford to wait and need to press ahead and invest in their own economies and security.

Whilst such a concept would have been considered the realm of conspiracy theorists in even the very recent past, the question as to whether the US can continue to be a reliable and trusted ally, both bilaterally and as the leading NATO member, is now being openly raised at top tables. Particularly given the US' recent willingness to throw around the use of economic weapons, such as tariffs, against allies and enemies alike, to force behaviours that support their interests.

The US government's unabashedly ebullient National Security Strategy(3) (NSS) and National Défense Strategy(4) (NDS) clearly articulate the approaches the administration intends to follow when applying the 'America First' doctrine to operate in its own core national interests. They demonstrate how the US plans to implement them in terms of exercising its own power and maintain hegemony in its relationships with its allies. This includes economic dominance and within that ensuring the dominance of US technical standards in AI, Biotech, Quantum, and Cloud, which the NSS states 'will undergird the US economy and strengthen its global influence'.

The impact of the Trump Corollary to the Monroe Doctrine (now sometimes referred to as the Donroe Doctrine) means that the US considers itself able to act with impunity in support of its own interests in 'its Hemisphere', which can be taken to include the whole of the Americas, as well as the traditional Western Hemisphere.

The transactional approach adopted by the US has inevitably reduced trust between the US and most of its allies, whether they are NATO members or not, and trust is, of course, absolutely fundamental to successful alliances. Furthermore, it is likely to mean that the basis of the 'special relationship' between the USA and the UK will be weakened over time, and that bilateral relationships can only be considered to be strong when they are in America's interests.

Whilst there is no doubt that Canada and European nations have not shouldered their full share of the costs of NATO, the lukewarm support offered to NATO in the NSS, is of significant concern to those nations and suggests that major changes are warranted, and not just in financial terms, particularly so when the NSS says that Europe faces 'the real prospect of civilisational erasure'.

As General Sir Richard Barrons said(5), post this year's Davos, this 'has sharpened the debate, it has affirmed that we are now dealing with a very different global security construct'.

It could be argued that, post the next US election in 3 years' time, things will return to 'normal', i.e. the Rules Based International Order will reassert itself, but once the polarisation genie is out of the bottle, it is difficult to see this occurring. Mark Carney, Lawrence Wong and others hold the same views.

This paper therefore argues that, whilst not abandoning traditional alliances and continuing to utilise US technology, the UK should also urgently invest to protect its 'crown jewels' in truly sovereign data centres, cloud, data analytic capabilities artificial intelligence (including generative AI), post quantum encryption, and, outside of tech, munitions manufacturing.

What does this mean for the UK and in particular UK Defence & Critical National Infrastructure?

For decades, since WW2, it has been taken as read by successive Governments that there is "a special relationship," between the US and UK, that transcends day to day politics. Consequently, over those decades, the UK has closely integrated its Defence, Intelligence and technology capabilities to those of its US partners and their supply chains. As detailed in the previous section, the geopolitical algebra has shifted and, in consequence, the UK should be carefully considering its future lines of action and conduct appropriate scenario planning.

One such area relates to Defence Industry. One of the key strategic lines of action in the NDS is to supercharge the US Defense industrial base. An underlying assumption being that as other NATO countries increase their budgets, so they will spend more on US kit and technology. As Gen Sir Richard Barrons recently said(5) 'many people – in and out of the MOD – are talking about how Europe, including the UK, will have to reduce its strategic dependence on the US. The US perception that we should spend more money on defence, but on US kit, is clearly ludicrous.

In response, the UK Government has recognised the need for a Defence Industrial Strategy (DIS), along with a Defence Investment Plan (DIP) to support the delivery of the recent Strategic Defence Review (SDR). However, the DIP has been repeatedly delayed and is now unlikely to be published until Easter 2026. Sadly, the SDR is not fully funded, although the Government has made the commitment to increase its defence spending to 5% of GDP by 2035. Many commentators, including the Chief of Defence Staff (6), are claiming that it is at least £28bn short and that this falls mostly in the early years. To supercharge the UK's defence industrial base will require a fully funded Defence Industrial Strategy and Investment Plan with both teeth and a determination to build sovereign capabilities in key areas

The immediate shortage of public money, especially in the early years of the defence plan, suggests the need for partnership between Government, industry and private capital. In the not-too-distant past, investors sought to steer clear of the Defence Sector, but this has now changed and the City of London could be mobilised to provide funding. The challenge for a Labour Government is that it was the Labour party that introduced the Private Finance Initiative as an off-balance sheet way of investing in infrastructure and, to say the least, this has not had a good reputation. Another challenge is that Defence would welcome an inflow of capital but would like to implement programmes themselves - industry would not welcome this! Notwithstanding this, there is an appetite in the City, which should be exploited.

The UK could learn from the US by establishing a focused technology investment organisation along the lines of In-Q-Tel. This would work alongside the Defence Investment Board but act like a commercial venture capitalist where agility, speed and engagement along with a much higher tolerance of risk and investment losses are key success factors. Such an approach can unleash the innovation often most prevalent in SMEs in support of the traditional primes.

This paper is not suggesting that a full decoupling from the US is warranted, rather that there should be a managed and prioritised migration from capabilities based upon US technology, services and suppliers, to an increased proportion of Sovereign capabilities. This should be augmented by bilateral and multi-lateral agreements (such as 5-Eyes intelligence sharing, AUKUS etc.) as appropriate.

Finally, on 5th February 2026 the world entered an epoch where there are no Treaties in force limiting the number and growth of nuclear arsenals. The last remaining bilateral nuclear arms control treaty between the United States and Russia, the New Strategic Arms Reduction Treaty (New START)(7) expires. Whilst there appears to have been recent informal agreement to extend the application of its terms by 6 months, this could contribute even further to geopolitical uncertainty.

The Technology Implications

US dominance of the Defence and National Security sectors is particularly apparent in the technology arena and especially so in the data space, be that around data centres, cloud fabric and services (e.g. Microsoft Azure, AWS, Google Cloud, Oracle Cloud Infrastructure plus many other service providers), data analytics (e.g. Palantir), and AI (e.g. Anthropic, Google, Open AI et al).

It has become increasingly obvious that technology is not neutral, it is subject to laws, politics and sanctions, such as the US CLOUD and Patriot Acts, which is driving greater focus on sovereign technology capabilities.

In light of this, many countries are beginning to consider what would happen if the US chose to limit or deny access to some of them in a future disagreement. Previously unthinkable, this is now a scenario that has moved from impossible to unlikely. Even though it remains unlikely, it is

a scenario that should be planned for, and, at a minimum, nations should therefore aim to keep their data 'crown jewels' in sovereign capabilities, to enable continued operations should such an event occur.

It is worth noting that in January 2026, the EU Parliament passed a 'Digital Sovereignty' resolution to support using public procurement to favour European Suppliers. This may be an approach that the UK may consider adopting in due course.

Furthermore, in a June 2025 hearing before the French Senate(8), Anton Carniaux, Microsoft France's director of public and legal affairs, admitted under oath that they cannot guarantee EU customer data will remain protected from U.S. government access, acknowledging that the U.S. CLOUD Act forces them to comply with data requests regardless of where the data is stored.

This testimony directly impacts trust in "sovereign cloud" partnerships involving U.S. firms. It has sparked intense debate regarding the "digital sovereignty" of using U.S. cloud providers, particularly for sensitive government and, "Health Data Hub" information.

The establishment of a government-wide policy of sovereign technologies, capabilities and suppliers considered to be critical to the UK, would be a great starting point. A secondary classification could include NATO allies, for instance in support of the Joint Expeditionary Force (JEF) and a third could include other strategic partnerships. This should include the establishment and ongoing operation of a supply chain intelligence capability. Maintaining situational awareness is key as new alliances and trade flows become established to augment or replace some of the 'pre-rupture' legacy ones.

Whilst some of the more favourable comments toward NATO in the NSS are encouraging to read, they appear to be based on the premise that despite all that has gone before, (including new tariff threats which do not exempt Defence), Europe and NATO allies will continue to be dependent upon American Defense and related technology capabilities. The US has proved to be less reliable and trustworthy and so whilst the UK should continue its bilateral arrangements it is also imperative that critical sovereign capabilities are established and maintained to meet the UK's needs as they may not always align with those of the USA. In such unforeseen circumstances support from the USA cannot be assumed or guaranteed.

Critical sovereign technologies, capabilities and suppliers

Eight areas for sovereign focus have been identified for immediate consideration, which are:

- data centres,
- cloud services
- artificial intelligence capabilities (including generative)
- data analytics at scale (especially at hyperscale)
- post quantum cryptography,
- telecommunications gateways
- telecommunications across the spectrum, and

- outside of tech and telco, munitions manufacturing.

Each area is discussed in more detail in the table below. These topics will be considered in greater detail in subsequent papers.

Data centres	More sovereign Data Centres are required to support existing and new technology capabilities including the development and hosting of sovereign AI capabilities at Official and possibly Secret. They should be constructed to Tier III / Tier IV standards as appropriate with the capability to implement physical and logically diverse connectivity for all services. Operational capabilities should include autonomous and 'smart hands' support. The positioning of sovereign data centres is critical. They must be able to be supplied with truly physical and logically diverse services, from electrical supplies through telecommunications to access for standby generator fuel resupply. Given their nature they will also be sited on much larger footprints to accommodate physical security requirements such as 'tank trap' perimeters.
Cloud Services	To be able to reduce dependency on the present group of Cloud Services Providers (e.g. AWS, Google, Oracle etc.) and to address the UK's data crown jewels, it is imperative to build sovereign cloud capability with functionality comparable to those hyperscale services at Official and Secret classifications. These capabilities should encompass all aspects of service provision, including, hosting (bare metal, containers and VMs), elasticity, scaling, orchestration, administration automation and CI/CD pipelines. Monitoring and billing of all elements of service provision is also a critical capability alongside those of Disaster Recovery & Business Continuity. For the avoidance of doubt these services will be designed to comply with current best practices and security and accreditation standards for Official and Secret trust domains. The cyber security requirements should not be overlooked. The technology infrastructure used to deliver the cloud services must be appropriately instruments to a granular level to be able to demonstrate compliance to accredited trust domain models as well as provide data feeds to agreed Cyber Security Operations Centres (CSOC).
AI capabilities (models, weights & training data)	Building sovereign AI models and capability so that organisational knowledge is not transferred to the models of third-party AI Service Providers (OpenAI, Anthropic, Google et al) who would otherwise have full access to that knowledge to analyse, share and exploit as they wish. This would also include the acquisition of Defence, Intelligence and CNI sector specific training data for these sovereign models.
Data analytics at scale	Building sovereign data analytics capabilities with the aim of matching those of the likes of Palantir over time and migrating public sector projects in Défense and elsewhere (such as the NHS) to these new capabilities when appropriate. This will also enable the UK to reduce its dependence on the use of Palantir over time.

	The acquisition of key data sets such as those created by Ukraine for drones and UAV's should be an imperative.
Post Quantum Cryptography (PQC)	Post Quantum Cryptography (PQC) is a discipline that aims to solve the issues that arise when quantum computing advances reach the point where todays encryption algorithms can be easily broken with Quantum Computers. It also aims to prevent "harvest now, decrypt later" threats. NIST has standardized algorithms like ML-KEM to protect against these threats.
Telecommunications gateways	Enhanced communications gateways' is a strategic capability. The UK has an opportunity to build more coalitions for more reasons with more partners. They'll want to work with us because they trust and rate us. That means we need a secure, repeatable, sovereign collaboration platform offering to help to support all of those. Unlike earlier approaches these gateways need to be comparatively inexpensive to build, deploy and operate to enable deployment at pace. They will be instrumented to ensure they can interconnect to appropriate Cyber Security Operations Centres for 24/7 monitoring.
Telecommunications (all spectrum)	The UK has become dependent on 3rd parties for many telecommunications services including GPS, PNT and satellite overfly services (LEO and geostationary). The reduction in dependence on these 3rd parties in favour of sovereign capabilities should be a priority although it is recognised this is a longer-term objective
Munitions manufacturing capabilities	The US has already articulated that it intends to increase its munitions manufacturing capabilities. If the UK is to be less dependent on the US in future and wishes to progress its own strategic defence initiatives, such as the supply of military equipment to Ukraine, it urgently needs to increase its munitions manufacturing capabilities.

Table 1 – Sovereign Focus Areas

Success will require each focus area in Table 1 to have a very senior sponsor to drive the initiatives forward.

Table 2, below, considers additional related activities which are necessary to deliver sovereign technology programmes and projects.

Government wide policies	The establishment of a government-wide policy of sovereign technologies, capabilities and suppliers considered to be critical to the UK, would be a great starting point. A secondary classification could include NATO allies and a third could include other strategic partnerships. This should include the establishment and ongoing operation of a supply chain intelligence capability. We should maintain situational awareness as things move fast and new alliances and trade flows become established to augment or replace some of the 'pre-rupture' legacy ones.
Gap analysis	A gap analysis should be developed to identify the technology, skills, systems and data impacts together with their reliance on non-sovereign suppliers and their capabilities to produce a prioritised program to close those gaps and/or manage the risks over time.
Strategic Plan	The output of the gap analysis together with agreed priorities will inform the scope, scale and delivery of the delivery projects. Interdependencies, their funding and timing will also need to be identified to ensure successful delivery of sovereign capabilities.

Increased focus on and participation in standards.	Participating in international standards bodies is essential if the UK is to influence their architectures and development. This was demonstrated when the PRC almost dominated the 5G working standards groups to push their own agenda to the detriment of many international participants. The UK needs to bolster its capabilities to be able to invest the time and effort to proactively participate in the development of technology standards and consequently their shaping. The UK will be respected and relied upon and more influential that way but we need to recognise this is a long-term activity that cannot be funded by an annual budget.
Architecture to enable delivery at pace	Interoperability and the ability to move at pace by 'swapping' capabilities and systems is a key enabler. To achieve this goal, it is essential that modular architectures are delivered that simplify systems design and delivery which in turn reduces complexity and cost and increases reliability and the ability to move with developments in technology as they occur, not years afterwards.

Table 2 – Related Activities

Other areas for consideration will be discussed in a follow-on discussion paper. They include:

- Development of inexpensive and highly effective drones and one-way effectors.
- Productivity & file sharing at Official and Secret security classifications
- Defence contracting
- Small & medium enterprises (SMEs) and their role in the supply chain
- Technical bench strength and the need to build it up to support sovereign capabilities
- Increased cyber security capabilities (defensive and offensive) in post 'rupture' and quantum worlds
- Intelligence sharing between allies and within NATO
- Oracle database dependency for key public sector service provision
- Procurement frameworks and making them more attractive and easier to use
- Venture funding and the role it could play to enable building more sovereign capability at pace

Calls to action

The world has changed; the old rules-based order is not returning. Allies previously thought to be totally trustworthy and reliable can no longer be so and therefore doctrine and policies need to be urgently updated to reflect this.

Consequently, it is imperative that the UK increases its sovereign capabilities for Defence and Critical National Infrastructure capabilities including their supply chains.

Given the preceding arguments, urgent action is required, driven by dynamic leadership in the following areas:

- Scenario planning should be undertaken for the 8 areas identified in Table 1 and informed by the areas identified in Table 2 ensuring their associated supply chains are included. Annex A highlights some working assumptions to underpin this activity.

- A fully funded Sovereign Capability Programme (CPP) should be mobilised, informed by scenario planning and tasked with further developing the UK's sovereign capabilities at pace as described herein.
- The scope of the CPP should also include the requirements of Critical National Infrastructure where there are overlaps and synergies thereby ensuring the requirements of Defence, National Security and the wider Critical National Infrastructure and their respective supply chains are addressed. In some cases, it is recognised that separate programmes outside of the CPP will be required, driven by respective stakeholders and their budgets.
- To address the immediate shortage of public money, especially in the early years of the defence plan, priority should be given to establishing a working partnership between Government, industry and private capital. Innovative ways to mobilise the City of London are required.
- The UK should establish a focused technology investment organisation along the lines of In-Q-Tel. This should work alongside the Defence Investment Board but act as a commercial venture capitalist. The inherent agility, speed and engagement, along with a much higher appetite for risk and investment losses, can unleash the innovation often most prevalent in SMEs in support of the traditional primes.
- In addition to the above:
    - Sovereign suppliers to Defence, National Security and Critical National Infrastructure together with innovative SMEs need to be urgently engaged and onboarded to facilitate delivery at pace.
    - Supply chains and their pipelines should be reviewed to identify and reduce / remove friction to enable them to deliver at pace too.
    - Commercial procurement processes should be reviewed to ensure they are aligned to the requirement to enable delivery at pace.
    - SME's should be enabled to apply to join procurement frameworks such as G-Cloud and Digital Outcomes and Specialists at any time, (not the 18-24 month periods currently the case) to facilitate easier SME access and make it more attractive to them to participate.
- Finally, the UK could seek to provide technological leadership to Canada and the European members of NATO, in support of initiatives such as the Joint Expeditionary Force (JEF) and any Stabilisation Force for Ukraine.

Annex 1 - Useful Working assumptions for Scenario Planning;

The following working assumptions have been used in the development of this paper: -

I. In the future, the US may no longer be regarded as a 100% reliable or trusted partner in Defence and Technology. US commitment to NATO cannot be assumed to be absolute or persistent under the current Trump and any future US administration. Cooperation with the US in existing areas of Defence, Intelligence sharing etc. will continue but will likely become more transactional over time as the US states clearly it will be more engaged when it is in their interests and less so elsewhere. The issue of burden sharing and simultaneity described in the NDS further supports this view but there is no description of how this may work in practice.

II. The US partially or fully withdraws from NATO. Given the statements in the NSS and NDS this does not appear to be likely, but with the unpredictability of President Trump and his administration it is a possible scenario that should now be considered. NATO would continue if the US withdrew but there would be a period of disruption as member states would have to increase their contributions to replace those lost from the US and new communications and lines of control would need to be established. From a Defence perspective, NATO countries are well integrated and whilst key capabilities provided by the US would be lost or diminished (intelligence sharing, satellite overflying etc.) the 'NATO First doctrine of member states' and interoperability of capabilities would enable it to continue, albeit initially at reduced levels. Such an action would also bring into question the presence of the only US nuclear early warning facility outside of mainland USA (Fylingdales) and the three airbases in the UK operated under USAFE-UK (RAF Fairford, RAF Lakenheath and RAF Mildenhall). These airbases have seen increased activity since the US intervened in Iran and in support of Israel (which country it describes, in the NDS strategy, as the "model ally").

III. Intelligence sharing within the 5EYES group will become more fractured or limited at times. Canada and the UK are already seeking to build stronger economic ties to the People's Republic of China. These closer ties to the PRC will not be looked upon favourably by the US administration because it conflicts with their global power ambitions, especially in constraining the influence of China as described in the NSS. Nor is it necessarily sensible, however other countries are doing the same with the PRC and other trading blocks, as they react to the economic headwinds resulting from President Trump's tariffs and look for other, more welcoming partnerships to sell their goods and services as well as establish new supply chains. President Trump has already said publicly that closer ties to Beijing is 'dangerous' for the UK.

IV. It should be assumed that under the 'America First' policy, that the The International Traffic in Arms Regulations (ITAR) regulatory framework (administered by the Department of State's Directorate of Defense Trade Controls (DDTC)) may be more rigorously and more widely applied to technology used by the UK and other NATO allies than has hitherto been the case.

V. Other US legislation that grants the Federal government and agencies sweeping powers, such as the PATRIOT Act could also be invoked without the knowledge of the UK or NATO allies.

VI. A sense of near fealty to the Trump administration amongst the CEOs and executives of many large US corporations of all types has emerged. Those who dissent are criticised and, in some cases, ostracised. The most recent example is that of Darren Woods the CEO of Exxon Mobil who publicly stated Venezuela was uninvestable. This statement incurred the wrath of President Trump. This situation is a concern as private agreements may have been entered into which are impactful but unknown.

VII. Dependency on US based Service Providers and technology suppliers should be reduced over time and sovereign capability bolstered in the areas of Defence and the support of Critical National Infrastructure and their respective supply chains. The UK cannot match their capability or scale, instead the UK should be focussed on providing alternatives that are high quality, compatible, and more sovereign, but necessarily narrower in scope, to enable more independence. This should include but not be limited to compute and 'supply chain' for all those data centres (as most of their internal infrastructure is likely to be supplied by Cisco, Dell, HP, etc.) and all of those could be just as easy to tariff too or have ITAR restrictions placed upon them. Critical software elements should also be included such as Virtual Machine, Container, Orchestration, Operations, CI/CD management and all other key software solutions used in the development and provision of cloud services.

VIII. Political pressure within the UK will likely result in more focus on partnerships with European partners, to the detriment of US partners, with NATO likely remaining the vehicle for that cooperation in Defence and its supply chains. A similar approach would likely be adopted for Critical National Infrastructure.

IX. A move towards closer ties to European partners will only be successful when the EU significantly slashes its propensity for legislation and over regulation. There is a phrase often used "America innovates, China replicates and Europe legislates". Whilst this is not at all a truism, the sentiment is close to reality. The EU was the first to trumpet to the world its AI Act, but the EU doesn't have any AI companies of note within the group, they are all in the US where the legislative and labour environments are more flexible, less constrained and more conducive to building fast moving scalable (internet scale) companies.

X. There is a risk that dependencies on the US become replaced by dependencies on European and other suppliers instead. Three members of the European Union (Bulgaria, Hungary & Slovakia) demonstrate at least some limited the Russian regime under President Putin. EU member states can still exercise vetoes in seven areas of competence, one being that of Foreign Policy and Security, which includes sanctions and Defence issues. It is assumed that the decision will be for the UK to have more sovereign capability independent of any European or other supplier. Clear strategies and policies

will be required to ensure appropriate support and investments are available from the public and private sectors.

XI. Mark Carney has already articulated that this new reality is a rupture, and his view appears to have gained widespread international support and so the UK should be incorporating this view into its doctrines, strategies and policies. A key working assumption is that we cannot and should not assume that the situation will return to as it was before President Trump was re-elected. It must be assumed that the ruptures remain and will continue with future US administrations. The damage cannot be repaired, and the situation will not return to as it was previously.

XII. Some existing and future capabilities (Trident, F35s, AUKUS etc.) will continue well into the future, uninterrupted due to the commercial and strategic significance to all parties.

References:

1. Mark Carney Speech at World Economic Forum, Davos, January 2026

https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada

2. PM Lawrence Wong in an interview with the Financial Times (Oct 2025)

https://www.pmo.gov.sg/newsroom/pm-lawrence-wong-in-an-interview-with-the-financial-times-oct-2025/

3. The National Security Strategy of the United States of America, November 2025

https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

4. The US National Defense Strategy 2026, published by the Department of War in January 2026

https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF

5. Financial Times article quoting General Sir Richard Barrons post Davos

https://www.ft.com/content/55af024b-7c09-4610-89e9-366f3f504dda

6. The Times newspaper interview with the Chief of the Defence Staff

https://www.thetimes.com/uk/defence/article/senior-military-chiefs-warn-keir-starmer-of-28bn-defence-shortfall-mb6pjkkl3

7. New START Treaty

https://www.state.gov/new-start-treaty

8. Transcript of Anton Cariaux's testimony to the French Senate

https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html