

Towards a UK-EU Partnership for a New Age

September 2026

Key points

A Valuable and Strategic Partnership

- **Deep Economic Integration:** The EU and UK share one of the world's most integrated digital economies, with bilateral trade in digitally deliverable services valued at over \$350 billion in 2024.
- **A Trusted Trading & Innovation Partner:** The UK serves as a vital source of strength and resilience, mitigating vulnerabilities that stem from the EU's heavy reliance on foreign firms, particularly those from the US and China, for ICT services and goods.
- **Critical to Security:** The UK is indispensable for continental defence, boasting Europe's largest cyber sector (with revenues over €10.3 billion in 2025), playing an essential role in addressing shared threats like cyber and hybrid attacks and underpinning digital trade.

The Risks of Divergence

- **Counterproductive Friction:** The current post-Trade and Cooperation Agreement (TCA) status quo and unilateral drives for technology sovereignty risk erecting new, counterproductive barriers between the two closely integrated jurisdictions.
- **Economic Costs:** The loss of automatic recognition of conformity assessments and passporting creates significant technical barriers and dual compliance costs, severely impacting small and medium-sized businesses (SMEs). Divergence also threatens the immense bilateral digital services trade.
- **Security Vulnerabilities:** Current friction has led to a de facto decrease in cyber information exchange and weakened collective resilience. Critically, the failure to structurally embed the UK in European defence instruments, such as the Security Action for Europe (SAFE), weakens the collective defence readiness and supply chain resilience.

Safeguarding Shared Prosperity: Key Actions for Policymakers

Defence & Security Resilience

- Urgently negotiate the UK's participation in European defence frameworks, such as SAFE.
- Strengthen cooperation on supply chain resiliency, cybersecurity, and digital infrastructure security through a trusted partnership model, closer alignment, and mechanisms for stronger information-sharing.
- Expand cooperation on dual-use emerging technologies (including AI, quantum, and autonomous systems) to align initiatives and strengthen collective security.
- Treat subsea cable infrastructure as a shared resilience priority, coordinating risk assessments, information sharing and security best practices across the full lifecycle of cable infrastructure.

Regulatory Interoperability & Dynamic Alignment

- Negotiate mutual recognition agreements in high-compatibility sectors to reduce compounding compliance costs for businesses.
- Maintain free and trusted data flows by advancing frameworks like the G7 Data Free Flow with Trust and promoting greater interoperability between data protection frameworks.
- Ensure AI and quantum regulatory interoperability, including cooperating on migrating to ETSI post-quantum cryptography standards and advancing the G7 Hiroshima AI Process.
- Maintain dynamic alignment for goods, especially in areas such as chemicals, product sustainability, labelling, and safety requirements, where divergence offers no benefits and imposes significant costs.

Digital Standards

- Maintain UK participation through BSI in the European Standardisation Bodies of CEN, CENELEC and ETSI and promote alignment through European and international standards that support interoperability, innovation and trade.
- Ensure personal and organisational digital identity interoperability.
- Harmonise AI, cybersecurity, and quantum technology standards to enable efficient compliance for industry.

Protecting Sovereignty

- Align on sovereignty initiatives and mutual recognition of trustworthiness in existing and upcoming proposals, such as the Cloud and AI Development Act.
- Treat public procurement as a tool for shared security and resilience by ensuring sovereignty and local content requirements are applied on a proportionate, risk based basis, with mutual recognition of assurance and compliance frameworks where outcomes are equivalent.

Introduction

Europe faces a new world.

The established norms and expectations of recent decades have been decisively turned on their head. The days where it was possible to hold out the hope of ongoing peace, increasing trade, and ever growing prosperity are gone and have been replaced by one marked by turmoil, sluggish growth, and existential threats. As President von der Leyen has argued, that old-world order “has gone and will not return.”¹

In this changed landscape, it is ever more important to build resilient and trusted partnerships. This is nowhere truer than in the case of the UK and the EU. Brexit introduced significant new barriers to trade and disrupted longstanding diplomatic and security cooperation between the UK and the EU. However, subsequent events have demonstrated how essential ongoing cooperation remains between both partners.

Russia’s war of aggression against Ukraine and the Covid-19 pandemic demonstrated the vulnerability of global supply chains. These have been joined by new threats to sovereignty and increased uncertainty from old allies.

Europe’s ambition for digital sovereignty is both urgent and legitimate. In an era of geopolitical tension, cyber threats, and rapid technological change, ensuring control over critical digital infrastructure is essential for security, resilience, and competitiveness.

But sovereignty cannot mean isolation. Rather, sovereignty must be built in partnership with likeminded allies.

This is made clear in the European Commission’s Technological Sovereignty Package.² The concept itself is rooted in “openness, partnership and fair competition. It does not mean isolation, protectionism, or tech decoupling.”³ President von der Leyen has also made this point, explicitly emphasising how “standing on our own feet does not mean standing alone. We also want to work with trusted partners around the world.”⁴

The EU and UK already share one of the deepest and most integrated relationships in the world, especially in technology, security, and digital economy. They also share the same geopolitical threats and challenges, and have a shared objective to reduce problematic dependencies in key technology supply chains, with new Prime Minister

Andy Burnham setting out his ambition for the UK to build more “sovereign capabilities.”⁵

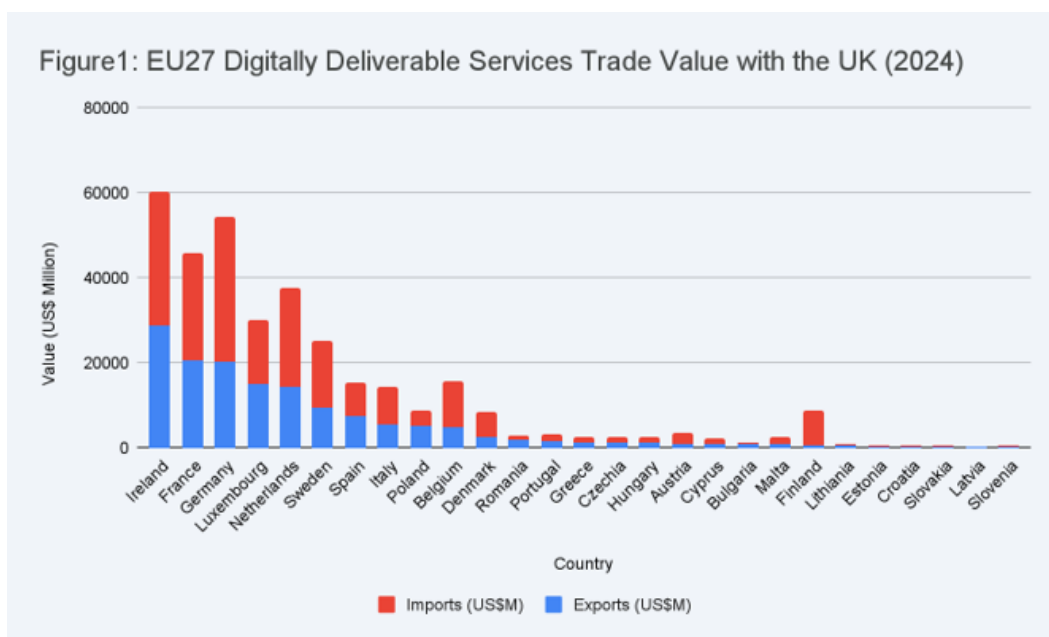
As the EU and UK look towards trusted-partner approaches to strengthen their sovereignty, both must ensure they look beyond just geography and corporate origin. Criteria for these partners must be transparent, proportionate and technology-neutral and must recognise robust governance, security, regulatory compliance and operational resilience. When these are taken into account, it should be clear that the UK and EU are essential partners for each other.



A valuable and strategic partnership

Decades of close collaboration and integrated supply chains have led to the EU and UK having one of the most valuable digital trade relationships in the world. The bilateral trade between the two in digitally deliverable services was worth over \$350 billion in 2024.⁶

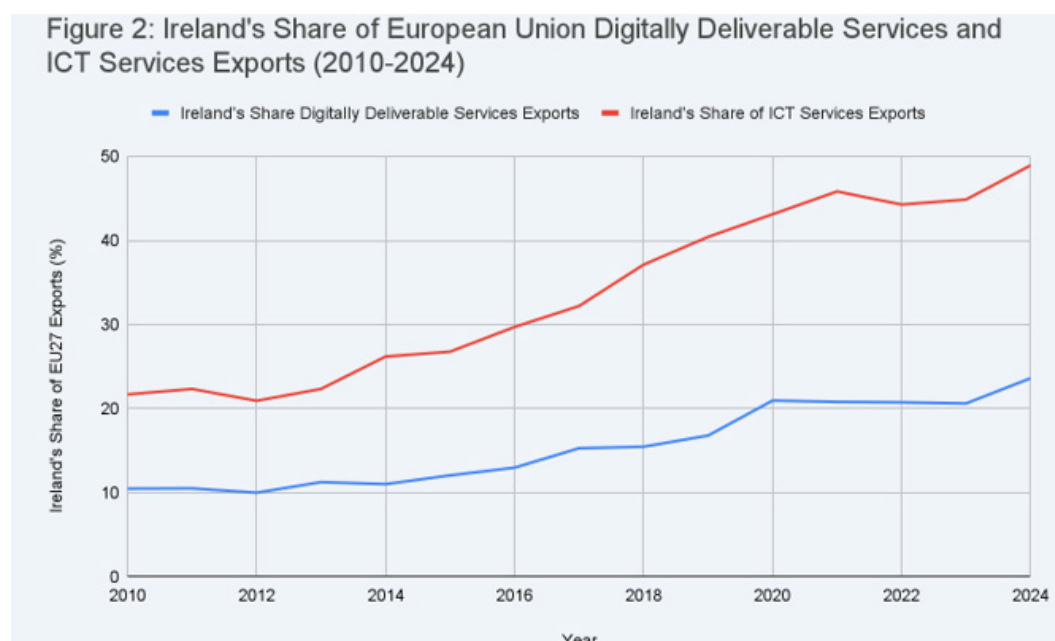
The UK is the number one non-EU export destination for digitally deliverable services for 11 member states, and is in the top five overall for 22 EU states—with the EU's total exports worth almost \$150 billion. Furthermore, the UK is an even more important source of digitally deliverable service imports, with EU members receiving \$203 billion in imports from the UK.⁷ [See Figure 1]



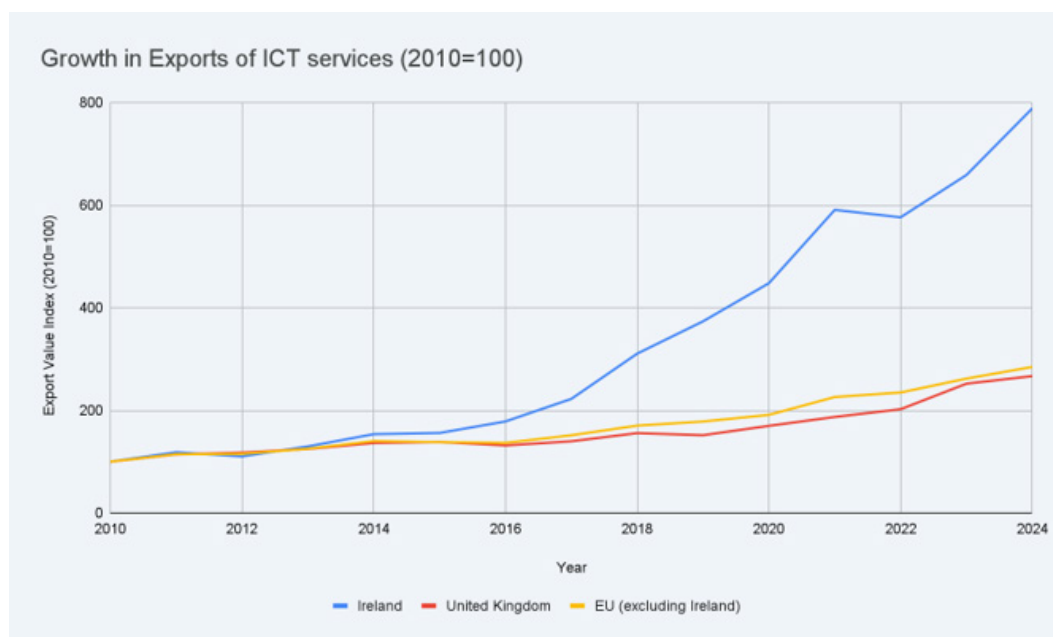
Source: WTO-OECD Balanced Trade in Services dataset, World Trade Organization,
https://www.wto.org/english/res_e/statis_e/gstdh_batis_e.htm

The UK is also Europe's single largest exporter of digitally deliverable services, with total global exports worth \$501 billion in 2024, second only to the United States of America. In comparison, combined the EU's 27 member states total exports of digitally deliverable services were worth \$1.9 trillion.⁸

While the headline figures demonstrate the scale of the EU digital economy, they should be interpreted alongside the significant contribution of multinational firms located in the EU, particularly in Ireland. A fuller assessment should distinguish domestic and foreign-owned value creation and consider the resulting benefits as well as concentration and dependency risks. Ireland's economy represented only 3.12% of the EU's \$19.5 trillion 2024 GDP.⁹ Yet, despite its small size, Ireland nonetheless exported 23.6% of the EU's total digitally deliverable services that same year—a figure that has been consistently rising over time. Ireland's disproportionate share of EU exports is even more starkly demonstrated when looking at ICT services exports in particular, where Ireland's share now accounts for almost half of the EU total.¹⁰ [Figure 2 & 3]



Source: "International trade in digitally deliverable services, value, shares and growth, annual (analytical)," UNCTAD, 2025-09-26, <https://unctadstat.unctad.org/datacentre/dataviewer/US.DigitallyDeliverableServices>

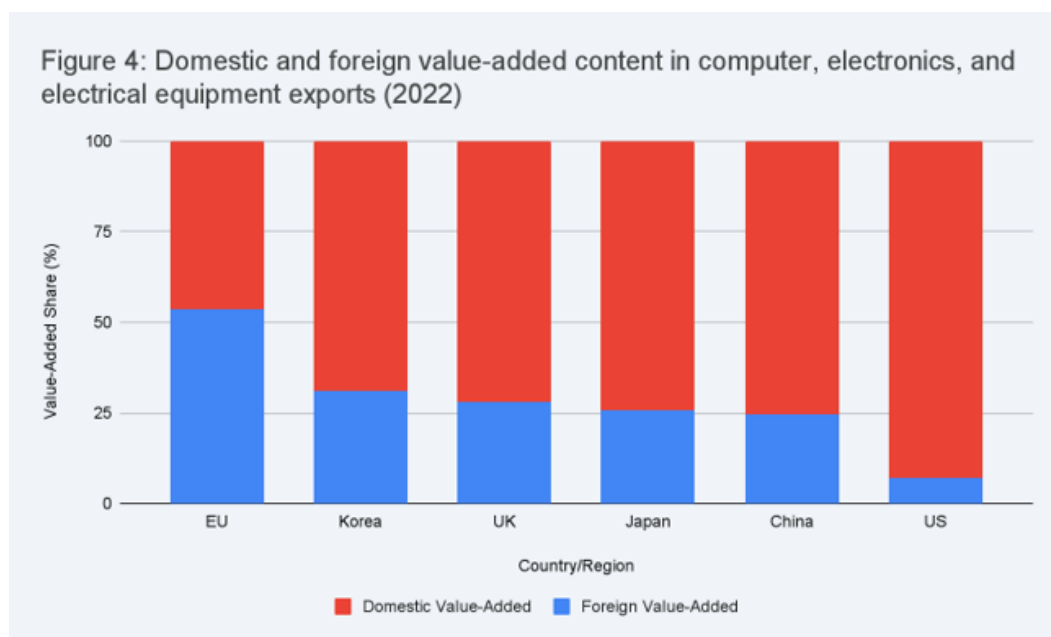


Source: "International trade in digitally deliverable services, value, shares and growth, annual (analytical)," UNCTAD, 2025-09-26, <https://unctadstat.unctad.org/datacentre/dataviewer/US.DigitallyDeliverableServices>

Recent analysis from the University of Bonn and the Vodafone Institute has highlighted the scale of Ireland's impact on the EU's digital trade, noting how without Ireland's contribution, the EU's digital trade surplus turns into a trade deficit. Furthermore, when it comes to value-added, Ireland's ICT sector "makes up a bigger share of total value created than all other European countries together in digital goods and digital services."¹¹

Ireland's inflated role in the EU's digital economy has been almost entirely driven by foreign, primarily US, firms. The Central Bank of Ireland has highlighted that as of 2021, 97.4% of gross value added and 93.9% of profits in Ireland's ICT sector were driven by foreign firms.¹²

In addition to the EU's reliance on the US for powering its digital service exports it is also exposed when it comes to the ICT goods trade. As the University of Bonn and Vodafone research indicates, the EU is the only global ICT leader where foreign-value added, exceeded the domestic value created, with China being the biggest source of ICT goods.¹³ Their conclusion is that, "as with the US and the Ireland effect, a high level of dependence on a single trade partner in ICT goods is a dependency that is already a vulnerability."¹⁴



Source: WTO GVC Sectoral Linkages taken from “Digital trade trap? A wake-up call for the EU’s Digital Decade,” Universität Bonn, 2026-03, p. 11, <https://www.vodafone-institut.de/wp-content/uploads/2026/03/wake-up-call-for-the-eus-digital-decade.pdf>

These figures speak for the important role the UK plays as a trusted trading partner of the EU. The deep interdependence and likeminded interests between the two are guarantees that the UK will not seek to leverage any dependency against the EU by cutting off access or restricting the supply of critical inputs. Nor will the UK engage in corporate espionage or unlawful access of European data. Instead, the UK is an important source of strength and resilience for the EU.

The UK’s significant innovation capabilities underscore this. The European Commission’s European Innovation Scoreboard notes how the UK is one of Europe’s innovation leaders. The UK outperforms 24 EU member states, and has been consistently improving its ranking, with a 12.2% increase in performance since 2018.¹⁵ Furthermore, the UK is home to 43 of the world’s most valuable tech companies, the equivalent to almost a third of the EU’s 156.¹⁶ The UK’s innovation strengths, paired with its economic weight—it has by far the largest economy out of European innovation leaders—mark it out as an essential partner for the EU.

The role the UK plays in boosting European strength and resilience is particularly acute when it comes to European security and defence. As a NATO and UN security council member, as well as one of Europe’s premier military powers, the UK is critical to continental defence. As the UK-EU Security and Defence Partnership sets out:

The UK and the EU share a responsibility for the security of Europe. The security and prosperity of the UK and the EU are also closely interconnected and interdependent. These shared



interests go beyond traditional strategic domains, to include areas such as cyber and hybrid threats, space, and the resilience of critical infrastructure. The EU and the UK share the same challenging security environment and both have vital interests in the peace, security and stability of Europe and beyond.¹⁷

Cybersecurity is an illustrative example of the importance of UK-EU digital and technology cooperation and collaboration. Cyber attacks on European critical infrastructure have reached new levels of intensity following the war on Ukraine. Russian attacks on Poland's power grid and a heating plant in Sweden demonstrate the threat posed by malicious actors on the everyday lives of Europeans.¹⁸ Indeed, cybersecurity researchers have gone as far as to emphasise how "Russian cyberwarfare threatens EU and UK security and democracy."¹⁹

The UK is a key part of Europe's cyber defences and UK cyber firms are longstanding contributors to the protection of European governments, businesses, and critical infrastructure, reflecting decades of close operational alignment and compatible approaches. The UK has by far the largest cyber sector, with revenues over €10.3 billion in 2025 and is expected to grow faster than all of its nearest competitors.²⁰ Furthermore, the UK has been an early, and substantial, investor in cyber with the first £860 million UK National Cybersecurity Strategy covering 2011–2016 being followed by £1.9 billion for 2016–2021 and £2.6 billion for 2022–25.²¹

The importance of the UK for boosting cybersecurity and European resiliency is further demonstrated by how cyber features as one of only two areas prioritised for thematic cooperation within the UK-EU Trade and Cooperation Agreement (TCA). Yet despite that, the TCA has nonetheless "brought about a de facto decrease in information exchange," that weakens practitioners' "capacity to understand the cyber insecurity landscape."²² Moreover, emerging "EU-owned and controlled" eligibility requirements for digital programmes are increasingly excluding trusted non-EU providers, including UK cyber firms, potentially weakening both European resilience and the foundations of a mutually beneficial UK–EU partnership.

The risks of divergence

The UK and EU are essential and irreplaceable digital and technology partners. The two provide complementary economic strengths that mitigate other vulnerabilities. Furthermore, their partnership is indispensable for European continental security. Unfortunately, as the cyber example illustrates, there is significant room to improve upon the current post-TCA status quo.

At a time when old alliances are being called into question and economic and security threats abound, it is an urgent imperative to strengthen the UK-EU relationship across all dimensions. Despite the scale of digital trade across the English Channel, the UK's position outside of the single market introduces barriers to trade that hamper the economic competitiveness of both sides. Failure to align digital and technology standards and supply chains, threatens both prosperity and security.

techUK members are clear about the importance of the UK-EU relationship. As one member said in an interview, "The UK is umbilically linked to Europe in terms of power, communications, and security infrastructure, and the two should be treated as an integrated system rather than separate entities."²³

techUK represents members who are headquartered in the EU in addition to those based in the UK. In reality though, many firms

have deeply integrated supply chains, customer bases, and legal corporate structures that span both. Geographic, commercial, and cultural ties still make this a natural arrangement. Expansion into the EU is "seen as a natural next step" by many UK tech businesses,²⁴ and the UK is often an early port of call for those from the EU.

This kind of expansion is made easier by substantial areas of convergence in the regulation of digital platforms and cutting edge services. These include topics such as online safety. While the Digital Services Act and the Online Safety Act have differences in their scope, approach, and the nature of enforcement, there is nonetheless fundamental alignment on the need to safeguard online environments in ways that are not shared globally.²⁵

Likewise, digital ID is an area where there is broad alignment in approach between the EU and the UK and a shared recognition of the potential for digital ID to offer access, convenience, and security to citizens. However, as the UK moves forward with the Digital Identity and Attributes Trust Framework (DIATF) and the EU advances the revised eIDAS framework it is going to be essential to ensure interoperability between the two. Divergence between the two will harm citizens and tech firms, given the highly interconnected nature of the digital ID ecosystem. The "ability to service international markets is



a key tenet for growth” for the UK’s ecosystem, with at least 30 UK headquartered firms serving the EU market and with many European digital ID businesses investing in the UK market.²⁶ A failure to ensure interoperability will undermine both.

The prospect of growing divergence and misalignment is a significant threat beyond the digital ID space. Geopolitical instability and renewed threats at home and abroad are placing pressure on the close integration of the UK and EU digital economies, as both seek to strengthen their strategic sovereignty. President von der Leyen has also described how her goal is to make Europe “more resilient, more sovereign and more powerful”²⁷ to be able to confront these challenges.

The EU and the UK’s sovereignty ambitions are based on legitimate concerns. However, members have stressed how “technology sovereignty is a double-edged issue.” In the view of some, it can be “a potentially counterproductive dynamic.”²⁸ Blunt restrictions risk erecting new barriers between two closely

integrated jurisdictions. This could have a range of negative impacts including, shutting British firms out of a €47bn sovereign cloud market by 2028, setting the template for AI, quantum, cyber and defence adjacent technologies, undermining UK outward investment already committed to EU based sovereign capable architecture, and triggering pressure for reciprocal UK restrictions, damaging UK–EU industrial cooperation. The end result would be to weaken collective European resilience and competitiveness, with UK capabilities, research, and innovation frozen out of critical digital infrastructures.

Efforts to strengthen sovereignty and resilience should recognise the deep alignment and commitments that exist between the EU and UK, from trade agreements to data adequacy decisions. Both should coordinate their pursuit of increased autonomy by adopting risk-based and proportionate approaches that seek to strengthen their control over digital infrastructures, while retaining openness to innovation and international cooperation. This will ensure that the EU and the UK continue to foster open

markets, and both remain globally competitive.

The risks of divergence are clearly illustrated in the failure for the UK to secure access to the EU's Security Action for Europe (SAFE), the financial instrument designed to speed up defence readiness. Despite the deep linkages and mutual dependencies in defence and security supply chains, the European preference means that EU members are prevented from procuring from the UK.²⁹ This impacts technologies such as the Franco-British storm shadow missiles which can only be bought using SAFE funds from their French and not their UK production sites.³⁰ Ensuring UK participation is an urgent task to secure sovereignty, resilience, and defence readiness.

Protecting digital infrastructure is another area of concern for members, who warned that diverging UK and EU approaches could “undermine trust and risk the UK being perceived as a security liability rather than an asset to European digital infrastructure.”³¹ Another member stressed the importance of the “UK and EU building mutual resilience in the face of current geopolitical shifts”, including through a more closely aligned approach to supply-chain resilience.

Another clear example of this is cooperation on the provision of satellite connectivity. Given the cross-border nature of satellite services, divergence between UK and EU 2GHz MSS frameworks would increase coordination complexity, reduce spectrum efficiency and weaken economies of scale. Divergence could also disadvantage UK operators by creating regulatory fragmentation and reducing opportunities to participate in a wider European MSS ecosystem. Aligning spectrum structures and authorisation approaches across the UK

and EU would support a larger, more investable market as well as enable more efficient use of the MSS band.

To avoid these risks, the UK should seek recognition as a trusted partner within the EU MSS framework. UK-headquartered companies should be eligible to participate in Category 2 award of spectrum (Commercial MSS systems for new Union entrants) where they meet the relevant security, resilience, and regulatory requirements. This would support investment and strengthen UK-EU cooperation in satellite connectivity, whilst ensuring that UK businesses are not excluded from one of their most important neighbouring markets of the EU.

Similarly, EU initiatives such as the “Cloud and AI Development Act” hold the potential to weaken European digital security and competitiveness if they unfairly discriminate against British firms and limit their ability to provide sovereign services to customers in the EU.³² For techUK members, such proposals reflect a “broader trend towards ‘digital sovereignty’ requirements within the EU”—an increasingly prominent concern for firms navigating regulatory divergence between the UK and EU.³³ Sovereignty measures should therefore be targeted at demonstrable risks and should not become a proxy for protectionism. Open, transparent and contestable procurement, supported by common assurance criteria and trusted-provider assessments, will strengthen resilience while preserving competition and innovation.

These requirements illustrate the broader costs of divergence, even where the UK and EU remain fundamentally aligned and share a high degree of mutual trust. For example, members have raised concerns that the loss of automatic recognition

of conformity assessments has created “significant technical barriers and dual compliance costs”, with a disproportionate impact on small and medium-sized businesses.³⁴ Another described how the loss of passporting meant that they and their clients had to be “compliant with fragmented local regulations rather than a single standard,” undermining services to EU businesses and consumers.³⁵

The issue of fragmented local regulations across EU member states is a particularly problematic one. That is especially the case given the existence of several overlapping EU-level regulations, such as the AI Act, Digital Services Act, Digital Markets Act, and General Data Protection Regulation (GDPR), and uneven enforcement. Recent research into the impacts of GDPR, for example, have found that both imports and exports of digital services with third countries have “experienced a significant decline” following the regulation’s introduction in 2018. However, it was not the existence of a data protection regime itself, but differences data transfer mechanisms that have driven these declines.³⁶ It is crucial to avoid measures that raise trade costs for companies. Regulators should coordinate implementation timetables, guidance and enforcement, and enable businesses to reuse verified information across compatible compliance regimes. This would reduce repeated data requests and preserve accountability while lowering costs, particularly for SMEs.





Safeguarding shared prosperity: Key actions for policymakers

The UK and EU are indispensable partners. Their relationship is foundational to the security and prosperity of the entire European continent.

Their digital economies are substantial and intertwined. With over \$350 billion in bilateral digital services trade, the UK is a vital source of strength and vitality to the EU's economy. Crucially, as a trusted trading partner that has the same fundamental values and faces the same threats, the UK helps mitigate vulnerabilities stemming from the EU's reliance on foreign digital and technology firms from the US and China. Beyond trade, the UK is also critical to continental defence and security, boasting Europe's largest cyber sector, and playing an essential role in military and security supply chains.

However, the current drive towards technology sovereignty posed risks of significant divergence that could undermine the strength and resiliency of both the UK and EU, if pursued through restrictive or discriminatory measures that limit market access for UK and EU companies. The failure to embed the UK within EU defence instruments such as SAFE, for example, weakens the resiliency of defence supply chains at exactly the time when Europe is more threatened than in generations. The UK must be included as a trusted partner within efforts such as the European Technological Sovereignty Package to avoid strategic disadvantage for both the UK and EU.

New barriers between the two closely linked jurisdictions risk duplication and

compliance costs that harm broader European competitiveness. These costs are already being felt. The loss of passporting and of automatic recognition of conformity assessments create significant technical barriers and dual compliance costs, especially for SMEs.

To safeguard shared prosperity and enhance the resilience of the wider European economy, policymakers in the UK and EU must act on their broader shared interests. There needs to be a renewed commitment to integration and alignment in areas where shared principles already exist.

A stronger, more constructive bilateral relationship between the UK and the EU is foundational to the sovereignty and prosperity of both. By working together both can translate their indispensable partnership into integrated resilience, securing a more stable and prosperous future for Europe.

1. Defence and Security Resilience

The UK and EU are essential for European defence and security. Both must take urgent steps to strengthen the partnership between them and deepen defence and security cooperation.

Include the UK in European Defence

Frameworks: It is an urgent priority to negotiate the UK's participation in defence readiness instruments such as SAFE.

Cooperate on Supply Chain Resiliency, Cybersecurity, and Digital Infrastructure

Security: The UK and EU have a shared interest in maintaining a common front on these issues, especially given the interlinked nature of European digital infrastructure. Strengthening

resilience and security, as well as continuing to build out next generation digital and telecommunications infrastructure, requires closer alignment and stronger mechanisms for cooperation between governments and industry on both sides of the English Channel. It is important to improve information-sharing, map existing risk assessment methodologies and certification frameworks, and identify practical opportunities to enhance interoperability and reduce unnecessary duplication. Both must ensure alignment on approaches to third countries and their risks to ensure there is no fragmentation between the UK and EU that could undermine security, nor slow down essential investment in connectivity.

Cooperation on cybersecurity and digital infrastructure security must be strengthened through a trusted partnership model that maintains mutual support for European security and resilience. This could include formal mutual recognition agreements for cyber security assurance schemes, conformity assessment bodies, and certification frameworks between trusted partners to avoid duplication and fragmentation. Such steps would ensure both jurisdictions can respond to cross-border risks at pace and scale, while preserving trust in shared digital ecosystems. The UK-EU Cyber Dialogue should be operationalised as the main delivery channel for practical cyber cooperation.

Expand Dual Use Emerging Technology

Cooperation: The future of defence relies on having an edge in key emerging technologies. AI and quantum are particularly important, as are drones and autonomous systems, space technologies, biotechnology, semiconductors, and advanced connectivity technologies. This is a space of intense competition, and both the UK



and EU members have invested significantly in these dual-use technologies, including through the UK's Defence Industrial Strategy and a planned £4 billion investment in uncrewed and autonomous military systems over the course of the current Parliament.³⁷ It is important for continental security that UK and EU dual-use technology initiatives are aligned and that they work together to strengthen the collective security of Europe.

Treat Subsea Cable Infrastructure as a Shared Resilience Priority: The EU and UK should approach subsea cable infrastructure as a shared resilience system, reflecting deep interdependence in digital connectivity and security. Implementation of the EU Action Plan on Cable Security should therefore be aligned with the UK, including coordinated risk assessments, information sharing and security best practices across the full lifecycle of cable infrastructure. This cooperation should also extend to NATO partners more broadly.

2. Regulatory Interoperability and Dynamic Alignment

Regulatory divergence between the UK and EU risks imposing huge costs on businesses and consumers. To avoid that outcome, both parties should negotiate mutual recognition agreements in high compatibility sectors to alleviate compounding compliance costs for businesses.

Protect Trusted Data Flows: Data flows underpin the UK-EU digital relationship, with European cloud-based data flows worth €77 billion to the EU and €22 billion to the UK in 2024.³⁸ It is important that the UK and EU maintain the free and trusted flow of personal and non-personal data between them and promote trusted data flows. This should include continued support for data adequacy, proportionate transfer safeguards and interoperable privacy frameworks, alongside reliable access to high-quality business data that enables customer and supplier due diligence, fraud prevention, anti-money laundering, sanctions compliance, credit assessment and

supply-chain risk management. In the context of digital protectionism, the UK and EU also need to work together to support and advance the G7 Data Free Flow with Trust agenda and support durable international rules for digital trade, while maintaining high standards of personal data protection.

AI and Quantum Regulatory Interoperability:

Both AI and quantum are increasingly critical technologies and it is important to act now to ensure there is no fundamental divergence between the UK and EU and that risks raised are effectively mitigated. Important steps include the need to cooperate on migrating critical infrastructure and sensitive systems to ETSI post-quantum cryptography standards. On AI, the UK and EU should advance the Hiroshima AI Process and its reporting framework as a common foundation for transparency, accountability and risk management. Different legislative models can coexist where they deliver comparable outcomes, use compatible definitions and documentation, recognise international standards, and avoid duplicative assurance obligations for organisations operating across both markets. A UK-EU AI Assurance Partnership should be created to facilitate alignment on those issues, including through greater cooperation between the AI Security Institute and the European AI Office.

Maintain dynamic alignment for goods:

In contrast, technology manufacturers value the ongoing dynamic alignment between the UK and the EU regulatory regime, given the deep linkages between the two markets. While on paper a divergent approach may appear to bring economic benefits, in practice it increases costs to business for no gain. Differing approaches to areas such as chemicals, product sustainability,

labelling, or safety requirements offer no benefits and should be avoided.

3. Digital Standards

From the development of trustworthy artificial intelligence systems or the emerging global rulebook for quantum technologies, stakeholders across the UK and the EU participate together in the development of over 30,000 European and international standards covering critical and emerging technologies which are vital to the continent's competitiveness and resilience.

The UK's participation in the European standardization system through BSI's ongoing membership of the European standardization bodies of CEN, CENELEC and ETSI is vital to ensuring continued alignment in the use of standards across the continent, including when it comes to those standards which support regulatory requirements. In addition, BSI is a strong voice, alongside fellow European national standards bodies for European interests in the international standardizing bodies of ISO and IEC, including in the global convergence of standards.

Ensuring interoperability of innovative systems across Europe through referencing the same standards in respective policies and regulatory frameworks is another important avenue to advance the UK-EU digital economy. The benefits for trade are even greater where the UK and EU mutually recognise accredited conformity assessments in cases requiring third-party verification.

Needless divergence in regulatory approaches, in those standards which are referenced in regulations as well as the non-recognition of conformity assessment results carried out in the other jurisdiction reduce trust between regulators,

impose duplicative compliance costs and reduce Europe's competitiveness, while alignment builds confidence and reduces barriers to trade through creating an enabling environment for one conformity assessment to serve both markets.

The UK's new Digital Standards Strategy rightly identifies the essential role that standards play in supporting economic growth, security, and prosperity.³⁹ It is encouraging that the Strategy recognises the importance of working closely with partners such as the EU that share the UK's values as well as share economic and security interests. Areas of important potential collaboration and partnership include:

Ensure Personal and Organisational Digital Identity Interoperability: As the UK advances its statutory digital verification services trust framework and the EU rolls out the revised eIDAS Regulation and EUDI Wallet, both sides should support cross-border recognition of trusted credentials for natural and legal persons. Building on the standards already common to both, such as ISO/IEC 18013-5, would let their credentials be recognised across borders. Beyond personal identification, cooperation should cover verified organisational identity, ownership and control, authority to act, and reusable business attributes, underpinned by privacy, security, data-quality and accountability safeguards.

Harmonise AI Standards: Although the UK and EU regulate AI differently, both rely on technical standards to make their rules workable. The EU's harmonised standards under CEN-CENELEC JTC 21 draw heavily on international ISO/IEC standards, including ISO/IEC 42001.⁴⁰ Coordinated engagement in CEN, CENELEC, ETSI and ISO/IEC should maximise the extent to which common standards, controls and

assurance evidence can be reused across both regimes, while recognising that applicable legal obligations remain jurisdiction-specific.

Harmonise Cybersecurity Standards: Given Europe's interconnected infrastructure, cybersecurity alignment is especially urgent. As the UK takes forward its Cyber Security and Resilience Bill, it should look to improve alignment with the EU's NIS2 Directive and progress towards mutual recognition. Where rules for high-risk third-country suppliers are introduced, both the UK and EU should take a common approach.

Align Quantum Technology Standards: Post-quantum cryptography is the most pressing task: with the first algorithms now standardised⁴¹ and the "harvest now, decrypt later" threat already live, the two should coordinate the migration of critical systems to ETSI post-quantum standards, and align emerging standards for quantum communications, sensing, and computing through bodies such as CEN-CENELEC's JTC 22.⁴²

4. Protecting Sovereignty

Underpinning all of these recommendations, it is essential that the EU and UK take steps to align their approaches towards, and understanding of sovereignty and of trusted partners.

Align on Sovereignty Initiatives and Mutual Recognition of Trustworthiness: As a baseline, both jurisdictions should recognise companies from the others' markets as trusted partners in existing and upcoming proposals (Cloud and AI Development Act, Public Procurement revision), and where sufficient controls are incorporated, as offering equivalent assurances to national companies.

Treat Public Procurement as a Tool for Shared Security and Resilience: As the EU revises its public procurement framework, both sides should treat public procurement as a tool for shared security and resilience, recognising the UK and EU as trusted and aligned markets for defence adjacent and security critical digital infrastructure. Sovereignty and local content requirements should be applied on a proportionate, risk based basis, with mutual recognition of assurance and compliance frameworks where outcomes are equivalent, to avoid unnecessary exclusions that weaken competition, resilience and supply chain diversity.



References

1. "Speech by President von der Leyen at the EU Ambassadors Conference 2026," European Commission, 2026-03-08, https://ec.europa.eu/commission/presscorner/detail/da/speech_26_576
2. "Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience," European Commission, 2026-06-02, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1187
3. "Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions on European Tech Sovereignty, accompanied by an EU Open Source Strategy," European Commission, 2026-06-3, <https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy>
4. "Speech by President von der Leyen at the EU Ambassadors Conference 2026," European Commission, 2026-03-08, https://ec.europa.eu/commission/presscorner/detail/da/speech_26_576
5. Andy Burnham, "We must rebuild Britain's hard power to face a darker world," The Times, 2026-07-08, <https://www.thetimes.com/uk/politics/article/andy-burnham-defence-nato-investment-rebuild-bc7rnr5l5>
6. WTO-OECD Balanced Trade in Services dataset, World Trade Organization, https://www.wto.org/english/res_e/statis_e/gstdh_batis_e.htm
7. WTO-OECD Balanced Trade in Services dataset, World Trade Organization, https://www.wto.org/english/res_e/statis_e/gstdh_batis_e.htm
8. "International trade in digitally deliverable services, value, shares and growth, annual (analytical)," UNCTAD, 2025-09-26, <https://unctadstat.unctad.org/datacentre/dataviewer/US.DigitallyDeliverableServices>
9. "World Economic Outlook (WEO)," International Monetary Fund, [https://data.imf.org/en/Data-Explorer?datasetUrn=IMF.RES%3AWE0\(9.0.0\)](https://data.imf.org/en/Data-Explorer?datasetUrn=IMF.RES%3AWE0(9.0.0))
10. "International trade in digitally deliverable services, value, shares and growth, annual (analytical)," UNCTAD, 2025-09-26, <https://unctadstat.unctad.org/datacentre/dataviewer/US.DigitallyDeliverableServices>
11. "Digital trade trap? A wake-up call for the EU's Digital Decade," Universität Bonn, 2026-03, p. 9, <https://www.vodafone-institut.de/wp-content/uploads/2026/03/wake-up-call-for-the-eus-digital-decade.pdf>
12. "Signed Article QB1 - March 2023," Central Bank of Ireland, 2023-03, p. 8, <https://www.centralbank.ie/docs/default-source/publications/quarterly-bulletins/quarterly-bulletin-signed-articles/the-role-of-ict-services-sector-irish-economy.pdf>
13. "Digital trade trap? A wake-up call for the EU's Digital Decade," Universität Bonn, 2026-03, p. 11, <https://www.vodafone-institut.de/wp-content/uploads/2026/03/wake-up-call-for-the-eus-digital-decade.pdf>
14. "Digital trade trap? A wake-up call for the EU's Digital Decade," Universität Bonn, 2026-03, p. 12, <https://www.vodafone-institut.de/wp-content/uploads/2026/03/wake-up-call-for-the-eus-digital-decade.pdf>
15. "European Innovation Scoreboard 2025," European Commission, 2025-07, p. 70, <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/c102236e-66b2-11f0-bf4e-01aa75ed71a1/language-en>
16. James Gree, "Europe Has Produced Tech Champions: Here Is What They Can Teach Us," Centre For European Reform, 2026-05-27, <https://mailings.cer.eu/insights/europe-has-produced-tech-champions-here-what-they-can-teach-us>
17. "Security and defence partnership between the European Union and the United Kingdom of Great Britain and Northern Ireland," Foreign, Commonwealth & Development Office, 2025-05-19, <https://www.gov.uk/government/publications/uk-eu-security-and-defence-partnership/security-and-defence-partnership-between-the-european-union-and-the-united-kingdom-of-great-britain-and-northern-ireland>
18. Milena Wälde, "Russia ramps up 'destructive' cyberattacks on Europe, says Sweden," Politico, 2026-04-15, <https://www.politico.eu/article/sweden-warns-russia-is-ramping-up-cyberattacks-on-critical-infrastructure/>
19. Lukasz Olejnik, "Russian cyber and information warfare and its impact on the EU and UK," King's College London, 2025-04-15, <https://www.kcl.ac.uk/russian-cyber-and-information-warfare-and-its-impact-on-the-eu-and-uk>
20. "The European market potential for cybersecurity products and services," CBI, 2026-02-19, <https://www.cbi.eu/market-information/outsourcing-itobpo/cybersecurity/market-potential>

21. Helena Farrand Carrapico, "UK-EU Cybersecurity Cooperation in the context of the Trade and Cooperation Agreement: implementation, impact and proposals for renegotiation," Independent Commission on UK - EU Relations, <https://static1.squarespace.com/static/6193d9441f87e0447a3f0803/t/639a063eda77e663c947f1e2/1671038531327/Independent+Commission+Cybersecurity+Paper.pdf>
22. Helena Farrand Carrapico, "UK-EU Cybersecurity Cooperation in the context of the Trade and Cooperation Agreement: implementation, impact and proposals for renegotiation," Independent Commission on UK - EU Relations, <https://static1.squarespace.com/static/6193d9441f87e0447a3f0803/t/639a063eda77e663c947f1e2/1671038531327/Independent+Commission+Cybersecurity+Paper.pdf>
23. techUK Member Interview #1.
24. techUK Member Interview #6.
25. Ashyana-Jasmine Kachra, Ayesha Gulley, and Siddhant Chatterjee, "Online Safety and the Digital Services Act (DSA): An Overview," techUK, 2023-07-10, <https://www.techuk.org/resource/online-safety-and-the-digital-services-act-dsa-an-overview.html>
26. "Digital Identity Sectoral Analysis 2025," Office for Digital Identities & Attributes, 2025-05-14, <https://www.gov.uk/government/publications/digital-identity-sectoral-analysis-report-2025/digital-identity-sectoral-analysis-2025>
27. "Speech by President von der Leyen at the EU Ambassadors Conference 2026," European Commission, 2026-03-08, https://ec.europa.eu/commission/presscorner/detail/da/speech_26_576
28. techUK Member Interview #2.
29. Alice Tidey, "UK defence industry calls for quick security pact with Brussels to access EU money," Euro News, 2025-09-04
30. Nicolai von Ondarza, "After SAFE: Consequences for EU-UK defence industrial cooperation and potential ways forward," UK In A Changing Europe, 2026-02-18, <https://ukandeu.ac.uk/after-safe-consequences-for-eu-uk-defence-industrial-cooperation/>
31. techUK Member Interview #1.
32. "Cloud and AI Development Act," <https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act>
33. techUK Member Interview #2.
34. techUK Member Interview #3.
35. techUK Member Interview #4.
36. Elena Sisto and Erik van der Marel, "Privacy at a Price? An Empirical Analysis of GDPR's Impact on EU Trade Flows," ECIPE, No. 11, 2025, https://ecipe.org/wp-content/uploads/2025/10/ECI_OccasionalPaper_11-2025_LY03.pdf. "Defence Industrial Strategy: Making Defence an Engine for Growth," UK Government, 2025-09-08, https://assets.publishing.service.gov.uk/media/68bea3fc223d92d088f01d69/Defence_Industrial_Strategy_2025_-_Making_Defence_an_Engine_for_Growth.pdf
37. "Data Flow and Economic Value EU Framework: Modelling Update and Data Collection," European Commission, 2024-03-26, <https://digital-strategy.ec.europa.eu/en/library/data-flow-and-economic-value-eu-framework-modelling-update-and-data-collection>
38. "Shaping Tomorrow: The UK's Digital Standards Strategy 2026-2030," UK Government, 2026-06-17, <https://www.gov.uk/government/publications/shaping-tomorrow-the-uks-digital-standards-strategy-2026-to-2030/shaping-tomorrow-the-uks-digital-standards-strategy-2026-to-2030>
39. "Artificial Intelligence," CEN-CENELEC, <https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/>
40. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," National Institute of Standards and
41. Technology, 2024-08-13, <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-Quantum-encryption-standards>
42. "Standardization Roadmap on Quantum Technologies," CEN-CENELEC, 2025-06, https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q06_standardizationroadmapquantumtechnologies_release1-1.pdf



linkedin.com/company/techuk



youtube.com/user/techUKViews



[@techuk.bsky.social](https://techuk.bsky.social)



info@techuk.org