
CYBER.
LONDON
Cyber & AI
Landscape Report
Innovation through Collaboration
NOT-FOR-PROFIT CYBER CLUSTER RECOGNISED
BY DSIT & SUPPORTED BY UKC3

OBJECTIVE

- Study the current Cybersecurity and AI landscape in the UK.
- Assess the objectives and outcomes of government-funded projects.(funding in cybersecurity and AI Only)
- Analyze initiatives led by accelerators, local cyber programs, and government bodies.
- Examine studies related to workforce and skills gaps in the cybersecurity and AI sectors.
- Identify gaps, duplications, and weaknesses in funding strategies and program execution.
- Provide strategic recommendations for more effective investment, strategic alignment, and structural improvements.
- Offer insights to help coordinate and streamline future efforts in cybersecurity and AI development across the UK.
- Projects in Cyber Physical (Cyber Grids, Defence, etc) is excluded from review.

APPROACH

Cyber Security Programs

- Program & funding review
  - Theme Wise
  - Sponsor Wise
- Cyber Local Program analysis
- Cyber Accelerators
- Academics and Certifications
- Diversity In Cyber Security Workspace
- Cyber Security Programs – Strengths and Weaknesses

AI Programs

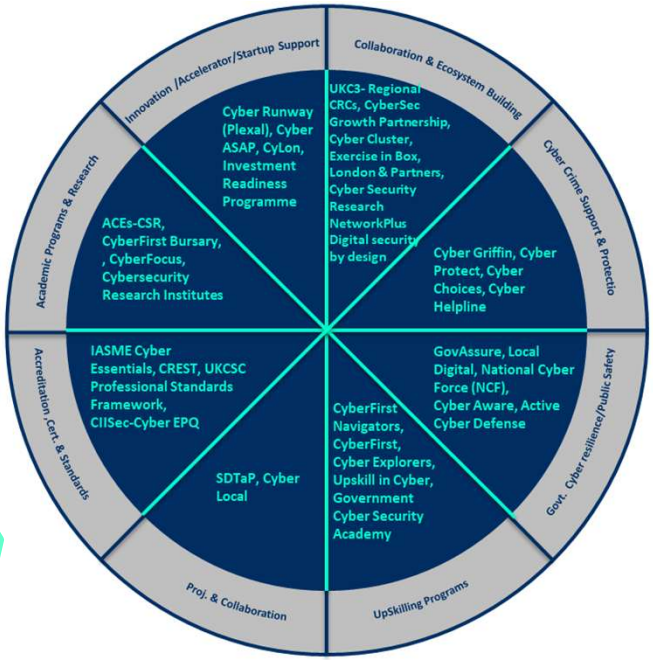
- Program & funding review
- UK EU AI Regulations Comparison
- Bridge AI
- Deep Dive
- Recommendations

Cyber Security Programs

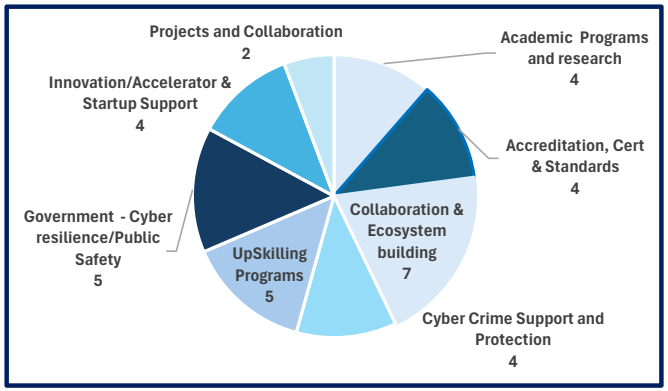
Program, Sponsor & funding review by Category

This slide evaluates 35 cybersecurity-related programs across 8 thematic areas, supported by 11 unique key sponsors, offering a comprehensive overview of the UK's national investment landscape in cyber initiatives.

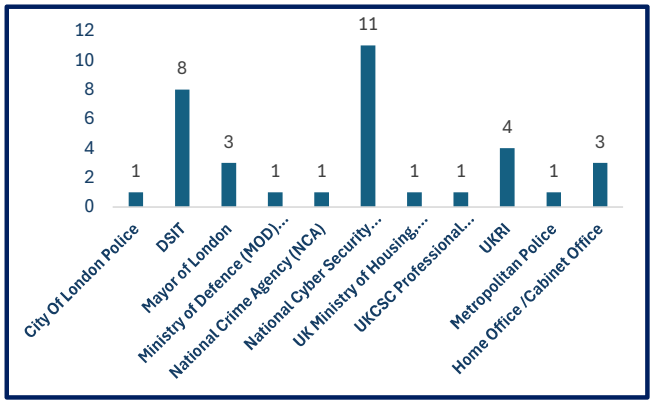
Program	Funding Detail
Cyber Helpline(2023-34)	£170K
UKC3 (2021-25)	£3.8m
Innovate UK - Cyber ASAP(2017-25)	£10m
Innovate UK-Cyber Local(2022-25)	£2.8m
Cyber Focus Initiative(One Time)	£4.9m
Cyber Security Research NetworkPlus	£6m
Cybersecurity Research Institutes(2023-26)	£7.5m
Security of Digital Technologies at the Periphery (SDTaP)	£30m
Plexal- Including Cyber Runway(2017-25)	£69m[1]
Digital security by design(2020-25)	£80m



Thematic Split of Programs



Sponsor* Wise Split of Programs

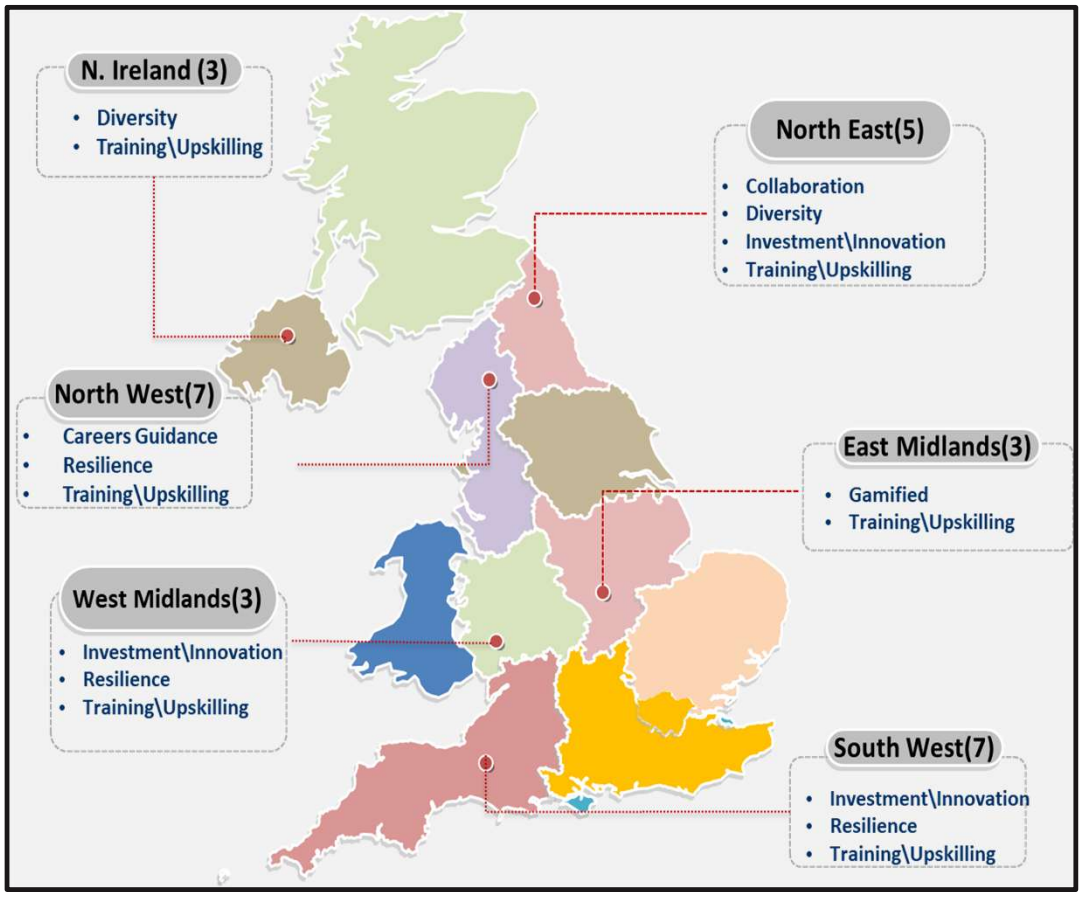


1.DSIT grant for Cyber Runway (2021-25)- £3.8m

* The split is shown by the primary sponsor. Additional Sponsors are not reflected in the chart

Cyber Local Programs (2024-25) – Deep Dive

Cyber Local – Regional Thematic Split



Innovate UK, part of UK Research and Innovation, will work with the Department for Science, Innovation and Technology (DSIT) to invest up to £1.8m (between £25,000 and £150,000 per project) in innovation projects across England and Northern Ireland.

Cyber Accelerators

	CyberASAP	Plexal Innovation + Associated Programs
Objective	Bridge the gap between academia and industry	Innovation company that designs and delivers accelerators, incubators, and innovation ecosystems
Operational Years	2017- Ongoing	2017-Ongoing
Projects	170 Academic Teams[3]	438 Core Programme Participants[1]
Grants Value	£10m	£69m[2]
Startups/Companies Registered*	34 Startups[3]	141 Businesses
Additional Funding Raised	Over £40 million[3]	Over £898 million.

1- Companies that have taken part in at least one core programme delivered by Plexal, including AWS Accelerators, and UK government-funded accelerators, including the London Office for Cybersecurity Advancement (LORCA), Cyber Runway, or NCSC For Startups.
2- 'Core' cohort of businesses have secured public and private grants, with a combined value of £69m through partners such as Innovate UK, MOD and Home Office. -Our impact – Plexal
3. CyberASAP

Academic \ Certifications – Deep Dive

Academic

NCSC Certified Degrees (Academic Centres of Excellence in Cyber Security Education - ACE-CSE)

Universities with high standards in cybersecurity education can become NCSC-certified, ensuring their degrees meet national criteria for academic and practical rigor.

NCSC CyberFirst (for Students Aged 11–21)

Offers a range of initiatives, including bursaries for university students, summer schools for teens, and apprenticeships.

- **CyberFirst Bursary:** Up to £4,000/year for undergraduates studying relevant subjects
- **CyberFirst Degree Apprenticeship:** Work-study option with government agencies
- **CyberFirst Girls** Competition and Courses for Schools

Apprenticeships in Cyber Security

Level 3 to Level 6 (degree apprenticeship)

Cyber EPQ: Level 3 qualification

Introduces students (ages 16–19) to real-world cybersecurity concepts through an independent research project.

Certifications

UKCSC Cyber Security Council Certifications

Currently building a professional chartered status for cybersecurity practitioners in the UK (similar to Chartered Engineers).

NCSC -Certified Cyber Professional (CCP) Scheme

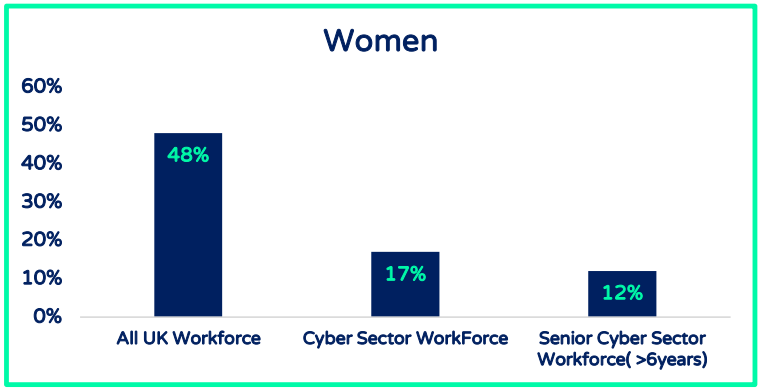
The CCP scheme is **delivered through approved** Certification Bodies (CBs) such as BCS, APMG, etc. Aimed at individuals working in cyber roles for government and critical national infrastructure. Requires high levels of knowledge, ethics, and competence.

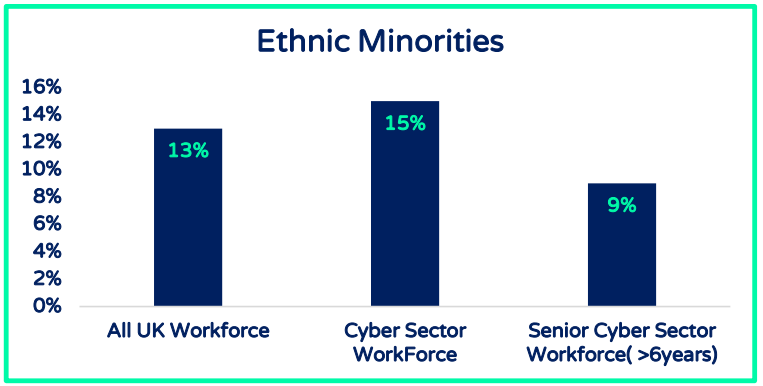
DSIT - Cyber Skills Immediate Impact Fund (CSIIF)

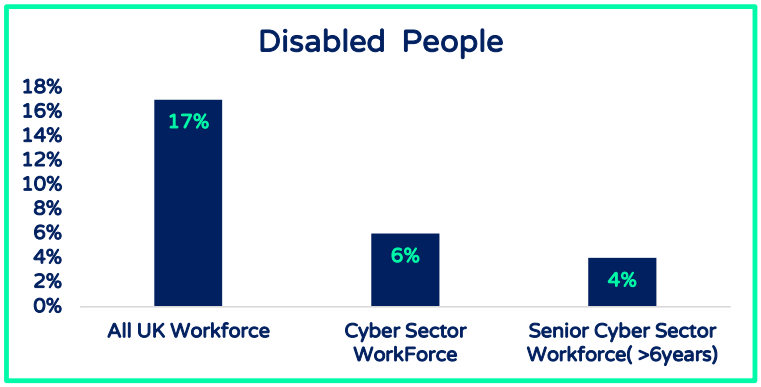
Funds training providers to offer free or subsidized cyber training to underrepresented groups or those reskilling.

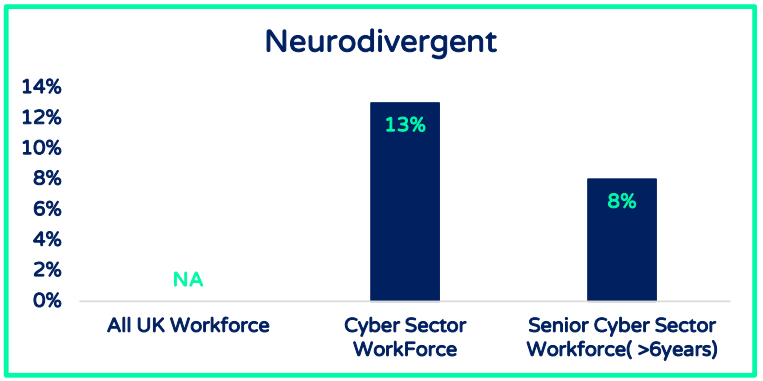
Diversity in the Cyber Sector Workforce

The UK cyber security workforce continues to face significant diversity challenges, despite growing recognition of the benefits of a more inclusive sector. The following data(as of 2024) highlights representation across key demographics—including women, ethnic minorities, neurodivergent individuals, and those with disabilities—offering insight into where progress has been made and where gaps persist.









Source: Cyber security skills in the UK labour market 2024 - GOV.UK

Strengths & Weakness

Strengths/Well-Covered Areas

Academic + Innovation Integration

Strong linkage between academia and industry via ACEs-CSR, Cyber ASAP, and CyberFocus. This ensures that research translates into commercial and security outcomes.

Startup & Accelerator Support

Accelerator support through Cyber Runway, CyberASAP combining previous fragmented programs (HutZero,, Cyber101, and Tech Nation's Cyber Accelerator). CyLon and others add additional layers for scaling.

Youth & Professional Upskilling

The CyberFirst ecosystem covers ages 11-17 and university students with bursaries, while programs like Upskill in Cyber and the Cyber Security Academy focus on adult and professional learners.

Ecosystem Development & Regional Growth

Programs like UKC3, CyberFocus, and Cyber Local reflect an emphasis on regional ecosystem building and partnership among public, private, and academic sectors.

Government Cyber Resilience

NCF, GovAssure, and Local Digital show strong attention to securing public institutions and departments through structured frameworks and governance.

Weakness/Gaps / Underdeveloped Areas

Post-accelerator Scale-Up Support

While startup accelerators exist, there's less visibility on scale-up funding, Series A/B bridging, or international growth support post-acceleration Startups: Duplication in funding, needs coordination

Private Sector Engagement Beyond Startups

Most business engagement targets startups or SMEs. Mid-size and enterprise-level cyber maturity development programs seem underrepresented.

Continuous Professional Development (CPD)

Upskilling focuses on early career transitions or youth. There is limited mention of advanced CPD or executive training for current cyber professionals. Fragmented training efforts

Impact Measurement Transparency

Although funding amounts and partners are mentioned, impact metrics (jobs created, breaches reduced, diversity stats, etc.) are rarely detailed.

Niche/High-Risk Sector Coverage:

Limited detail on cyber initiatives tailored to NHS/healthcare, manufacturing, defense suppliers/critical infrastructure, or education sectors specifically. These are critical yet high-risk verticals.

Underrepresented Demographics

Cybersecurity programs lack sustained inclusion of underrepresented groups—women, minorities, neurodiverse, LGBTQ+, disabled, older adults, and non-STEM individuals—leading to poor retention and limited diversity across education and career pathways.

Summary – Inefficiencies, Duplication & Gaps - I

1. Duplication in the efforts of Accelerator Programs

Plexal runs a stream of "core programs" supporting cyber startups through initiatives like Cyber Runway and LORCA(London Office for Rapid Cybersecurity Advancement). Separately, **CyberASAP** connects academia with industry to commercialize research, offering overlapping support in mentorship, validation, and early-stage growth. This parallel structure risks duplication of efforts, resources, and partner engagement. Streamlining both into a unified innovation pipeline could enhance efficiency and impact.

2. Fragmented Upskilling Efforts

Upskilling efforts in the UK cyber ecosystem are fragmented across multiple initiatives like **CyberFirst** and various **Cyber Local programs**. These programs often target overlapping groups with similar content but differing formats, leading to inconsistency and inefficiency. A more consistent, streamlined national framework would reduce redundancy and ensure better reach. Rather than designing multiple new programs, core cyber literacy and skills training should be embedded in mainstream school education to build a sustained talent pipeline.

3. Parallel Regional Projects

The '**Cyber Local**' program funds numerous regional initiatives intended to boost local cyber capabilities. However, without centralized coordination or a national delivery framework, these efforts risk duplication—multiple regions may develop similar programs independently. At the same time, some areas may miss out entirely, leading to uneven access, inconsistent quality, and unequal impact across the UK. A more cohesive strategy could ensure broader coverage and better resource optimization.

Summary – Inefficiencies, Duplication & Gaps - II

4. Complex UK Cyber Certification Pathways

The UK's cybersecurity certification pathways are complex due to a fragmented ecosystem of qualifications, including NCSC-certified degrees, UKCSC Chartership, CISSP, and the Cyber EPQ, each with specific purposes and prerequisites. The variety overwhelms learners, who struggle to choose appropriate certifications without clear guidance. Stringent requirements, like years of experience for CISSP or endorsements for UKCSC Chartership, exclude early-career or non-technical individuals. The transition from NCSC's Certified Cyber Professional scheme to UKCSC Chartership adds uncertainty, requiring professionals to adapt to new standards. The Cyber EPQ, while accessible, lacks clear progression to advanced certifications, complicating career planning. A lack of centralised guidance further confuses learners and employers, hindering effective navigation of the system.

5. Insufficient Support for Underrepresented Groups

There is a significant lack of sustained support and targeted programs for women, ethnic minorities, and neurodiverse individuals within the cybersecurity field. This lack of support is reflected in the underrepresentation of these groups in both the general workforce and at senior levels. Despite growing awareness of diversity's importance, the absence of mentorship, career development initiatives, and inclusive hiring practices prevents these individuals from entering the industry and advancing to leadership roles. As a result, the cybersecurity sector continues to lack the diverse perspectives and experiences necessary to drive innovation and progress.

Summary – Inefficiencies, Duplication & Gaps - III

6. Lack of Impact Measurement

Many cybersecurity initiatives—ranging from skills training and academic programs to research and startup funding—are launched with good intent, but often lack a consistent and transparent framework for measuring their effectiveness. Without clear metrics or evaluation standards, it becomes difficult to assess the real-world impact of these investments, compare program outcomes, or determine which initiatives deserve continued or increased funding. This absence of coordinated impact measurement hinders strategic planning and accountability across the ecosystem.

7. Neglected High-Risk Sectors

Critical sectors such as healthcare, manufacturing, and education remain vulnerable to cyber threats, as most funding in these areas is primarily directed toward digitalisation efforts, with limited focus on cybersecurity. This imbalance leaves essential systems exposed, despite their high-risk nature and increasing reliance on digital infrastructure.

Recommendations

Government-Level Alignment

- Streamline overlapping cybersecurity initiatives across government departments to reduce duplication, improve efficiency, and ensure consistent, high-impact delivery. Multiple sponsors currently fund similar efforts without coordination, leading to fragmented outcomes.

National Coordination Framework

- Establish a unified framework that connects government, industry, and academia, enhancing transparency, reducing costs, and driving consistency and scalability across the UK cybersecurity ecosystem.

Enhance Support for Scale-Ups

- Introduce targeted funding, growth accelerators, and infrastructure support for cybersecurity scale-ups to bridge the gap between early-stage innovation and mature commercial deployment.

Strengthen Industry Engagement

- Incentivize deeper collaboration among SMEs, large enterprises, and cyber innovators through innovation sandboxes, co-funded pilot projects, and procurement pathways that promote the adoption of emerging technologies.

Recommendations

Expand International Market Access Support

- Develop export readiness and international expansion programs for UK-based cybersecurity firms, including market intelligence, partnership facilitation, and government-backed soft-landing hubs abroad.

Improve UK Entry Support for Global Firms

- Launch a national onboarding and mentorship initiative for international cybersecurity companies seeking to establish a presence in the UK, providing business development support, legal guidance, and connections to local innovation ecosystems.

Create Dedicated Mentorship Networks

- Build structured mentorship programmes tailored for SMEs and international entrants, connecting them with experienced industry professionals, investors, and policy advisors to accelerate market integration and growth.

Invest in Mid-Career and Executive Cybersecurity Leadership Programs

- Fund and promote advanced training pathways and executive-level development programs aimed at mid-career professionals and senior leaders to ensure a pipeline of experienced cybersecurity leadership in both the public and private sectors.

AI Programs

AI Funding – Focus Areas

AI Research and Development

- **Alan Turing Institute**: Core of academic AI research. Focused on applying AI in sectors like health, defense, and environment.
- **AI Opportunities Action Plan**: A broader initiative to shape the AI market and drive socioeconomic impact.

AI Safety and Security

- **AI Safety Institute (Security Institute)**: Positioned as a global leader in AI safety evaluations.
- **AI Security Lab + LASR (GCHQ/NCSC)**: Focused on national cybersecurity, especially against AI-augmented threats.

Industry and SME Adoption

- **BridgeAI Projects**: £32M and £7M funds dedicated to driving adoption in public services and SMEs.
- **BridgeAI Innovation Exchange**: Small but targeted effort toward high-growth accelerators.
- **Digital Catapult**: Fosters practical AI use by linking startups and industry.

UpSkilling

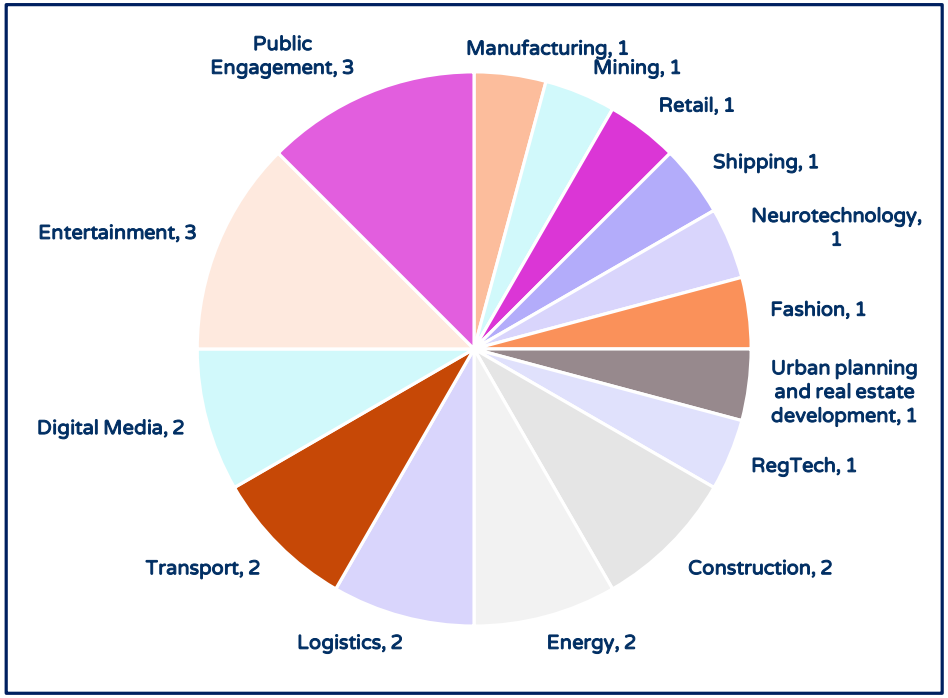
- **DSIT's Flexible AI Upskilling Fund** aims to bridge the skills gap, specifically targeting SMEs in the PBS sector. With £6.4 million earmarked for grant funding, eligible businesses can now apply for assistance to cover up to 50% of their AI training expenses..

AI Bridge Program – Cohort 1,2 &3

Innovate UK's **BridgeAI** program is to help UK businesses harness the power of AI by bridging the gap between AI developers and industry to drive innovation and productivity.

Thematic Split of AI Bridge Programs Cohort - 1 to 3

Theme	Count
Manufacturing	1
Mining	1
Retail	1
Shipping	1
Neurotechnology	1
Fashion	1
Urban planning and real estate development	1
RegTech	1
Construction	2
Energy	2
Logistics	2
Transport	2
Digital Media	2
Entertainment	3
Public Engagement	3
Grand Total	24



UK Vs EU AI Regulation–At a Glance

Category	EU AI Act	UK AI Approach	Gap Highlight
Principal	Regulation, Trust, and Innovation	Five core cross-sectorial principles	Safe, Secure & Robust, Appropriate Transparency Fairness, Accountability & Governance, Contestability & Redress
Regulatory Style	Centralized law	Decentralized guidance	UK lacks a unified framework, relying on sector-specific guidance.
Risk Framework	4-tiered (high to minimal)	No, principle-based	EU provides detailed categorization; UK is more interpretive.
Foundation Model Rules	Yes	Not yet	UK has not formalized foundation model governance.
Enforcement	Strong, with fines	Light-touch, sector-led	EU imposes penalties; UK depends on voluntary compliance.
Innovation Focus	Encouraged but regulated	High priority	UK is more pro-innovation, potentially at the cost of oversight.
Surveillance Rules	Very strict	More flexible	UK allows more leeway in surveillance applications.
Status	Finalized (phased rollout)	In development	UK is lagging behind in finalizing its AI policy.

Policy Area	EU Focus	UK Focus	Gap Highlight
AI for Climate & Sustainability	High	Low	UK has minimal focus on climate-related AI policy.
Ethics & Legal Alignment	High	Low–Medium	Ethical and legal frameworks stronger in the EU.
Rights-based AI	High	Medium	UK shows less emphasis on individual rights protections.
Civic / Public-Interest AI	Medium	Low	UK lags in fostering public-interest applications of AI.
AI Literacy & Worker Support	Medium	Low	EU supports education and workforce transition more robustly.

Artificial Intelligence – Q&As
EU AI Act: first regulation on artificial intelligence | Topics | European Parliament
https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf
Legislating AI: A Comparison Between the EU and the UK
UK vs EU Approach to Regulating AI: From One Extreme to Another? - Baker McKenzie InsightPlus

AI Program – Analysis

Overlaps Identified

Overlaps	Programs Involved	Comment
AI Security & Safety	AI Safety Institute, AI Security Lab, LASR	All work on similar problems. Potential for redundancy unless tightly coordinated.
Innovation/Accelerators	BridgeAI, Digital Catapult, Innovation Exchange	All engage startups but may compete for the same pool of participants.
Public Sector Efficiency	BridgeAI £32M, AI Opportunities Action Plan	Risk of duplicating efforts in AI adoption across public services.

Missed Opportunities

Area	Comment
Creative Industries & Media	Little targeted support for AI in arts, design, gaming, or entertainment.
Education & Upskilling	No large-scale program dedicated to building a future AI-ready workforce (outside of ad-hoc Turing initiatives).
Consumer AI & Ethics	Most initiatives are enterprise or defense-oriented — fewer focused on ethical implications of AI in everyday life (bias, accessibility).
Startup Scaling Support	Funding exists for initial R&D but few tailored programs help AI startups scale internationally.
Data Infrastructure	No major program focuses on developing open, trusted datasets — a key enabler for innovation and fairness.

Strengths/Well-Covered Areas

- **Diverse Stakeholders**
  Involves academia, SMEs, corporates, and government agencies.
- **Safety Leadership**
  Early investment in AI safety (e.g. Safety Institute, LASR) positions UK globally.
- **SME Focus**
  Specific funding streams for small businesses (BridgeAI £7M).
- **Geographic Spread**
  BridgeAI projects delivered across the country/ regional inclusivity.
- **Multi-sector Impact**
  Programs target sectors like healthcare, public admin, defense, and environment.

Weakness/Gaps/Underdeveloped

- **Lack of Cohesion**
  Overlaps and parallel programs (e.g., Safety Lab vs LASR) can dilute impact.
- **Modest Scale**
  Some funding levels (e.g. Innovation Exchange £200k) are relatively small-scale.
- **Limited Commercialization Pipeline**
  Missing structured follow-through from R&D to deployment, especially for SMEs.
- **Unclear Metrics**
  Many programs lack transparency around KPIs, evaluation frameworks, or public reporting.
- **Over-emphasis on Risk/Defense**
  Strong on AI safety but weaker on nurturing consumer/creative AI applications.

Recommendations

Scale Up Funding and Consolidate

- **UK funding is modular and modest. Compared to EU Horizon Europe , UK efforts feel fragmented.**
- **There's an opportunity to bundle programs into larger, impact-focused missions (e.g., AI for Net Zero, AI for NHS, etc.) bigger and more integrated** (coordinated funding blocks). Launch **mission-driven initiatives** (AI for NHS, climate, transport).

AI in Education, Workforce & Public Services

- **No flagship programs focused on:**
  AI upskilling and education pipelines (except some pilot DSIT Program - he DSIT's Flexible AI Upskilling Fund).
  AI for schools, local councils, or NHS transformation at scale.

Commercialisation & Global Scaling

- **UK startups often stall at Series B/C. There's a "valley of death" between academic R&D and export-ready productisation.**

AI, Ethics & Inclusion

- Need more effort around:
  - **AI for accessibility, bias reduction, digital inclusion**.
  - Supporting creative industries with AI tools (e.g., music, gaming, design).

Strategic Compute Access

The UK lacks a **nation-scale compute infrastructure** (compared to France's **Jules Verne**, Germany's **LEONARDO**, or US/China hyperscale GPUs). Build **national infrastructure** for computing and data.
The UK has announced a **Frontier AI Taskforce** and **Isambard-AI supercomputer but** needs faster rollout and wider access.

Thank You