

OCTOBER 2024

Lancaster University

Developing the North West Cyber Ecosystem



01 Foreword

//

If we all continue to work together with our partners, we are convinced that we can make the North West the leading region in the country for cyber innovation and investment.

From MIT research, it is clear that innovation follows a place-based ecosystem logic. Such tech innovation does not just happen spontaneously or in random places, but in ones with the right local capacities, and especially with five key stakeholders who collaborate.

It is the stakeholders' human agents – finding ways to cooperate despite their varied perspectives – that make the difference. This multi-stakeholder ecosystem logic is as true of cyber security, as it is of biotech, cleantech, and 'dual-use' technologies for security and defence¹.

That is why MIT supports the North West Cyber Ecosystem approach, and attended the CyberCom Event in Lancaster, which not only brought together all five key stakeholders, but a range of talents in each group. This is just the sort of initiative that can give a region a competitive advantage, and the North West is well-placed to support and make the most of the UK's National Cyber Force (NCF) moving its HQ into Samlesbury, Lancashire.

DR PHIL BUDDEN
MIT REAP

'Developing the NW Cyber Ecosystem' was a unique event to bring together over 60 delegates from universities, government and industry with innovation specialists and risk capital investors from the North West. Each delegate represented one of those five stakeholder groups critical to the successful adoption of MIT's Regional Entrepreneurial Acceleration Programme (REAP).

It was fitting that the delegates benefitted from an inspiring keynote speech from one of the programme's architects, Dr Phil Budden.

The good news is that the North West is starting from an enviable position; the North West Cyber Ecosystem is currently the largest in the UK after London and the South East and has the potential to nearly triple in size over the next decade.

One of the main aims of this event was to provide an opportunity for the stakeholder groups to get together and discuss the key challenges that each one of them faced in taking the ecosystem to the next level. This document distils those discussions into the crucial principles that we need to take forward – the importance of collaborative and strategic focus, the need for cohesive partnerships and interventions, the critical role of our universities, the significance of place-based funding and the need for inclusivity and vision in developing the skills pipeline for growth.

The indicators are already overwhelmingly positive – the North West now has 350 cyber security businesses compared to 300 in 2023 and 55% of the investment in the UK cyber ecosystem in the first half of 2024 has been in the North West. However, there are ongoing global challenges that we continue to face, such as a highly competitive labour market, increasing market competition to secure inward investment and a widening cyber threat landscape. In that context, this document plays a highly beneficial role in unlocking for us the most important next steps that we need to take to fulfil the game-changing potential for the growth of the North West Cyber Ecosystem.

We are grateful to Research England and their CCF-RED programme for funding this activity to support pump-priming of university collective capabilities for commercialisation of research and knowledge, including collaborative R&D with business and innovation ecosystem development.

PROF SIMON COOK
LANCASTER UNIVERSITY

¹MIT, Global EPIC (2021) Cybersecurity, Innovation, and Regional Ecosystems (A Comparative Study): Available at: https://innovation.mit.edu/assets/MIT-GE-EPICfinal_April-2021_FINAL-2.pdf

02 Background

In Summer 2023, Lancaster University and Plexal published the **North West Cyber Corridor Innovation Impact Study**. This research found significant evidence underpinning the strengths of the cyber security ecosystem in the North West, including that the region hosts the second largest cyber cluster in the UK, with over 300 unique cyber security companies, and a well-established cyber ecosystem. It also found that there is an estimated c.12,000 FTEs working in cyber security in the NW generating £760m in Gross Value Added (GVA) each year, with potential to grow this to at least 30,000 FTEs by 2035 - unlocking up to £2.7bn in GVA for the region each year.

In May 2024, Lancaster University hosted a collaborative event with MIT as part of the North West Cyber Security Connect for Commercialisation (NW CyberCom) project¹, a £1.2 million project funded by Research England aiming to unlock the cyber security potential of the North West. This project seeks to partner with entrepreneurs, investors, government, and businesses to transform cutting-edge knowledge into innovative new products, services and policy, to better protect consumers, businesses and UK infrastructure.

This **Developing the North West Cyber Ecosystem event** convened over 60 delegates from the North West ecosystem across five key stakeholder groups: government, universities, corporate, investors, and entrepreneurs. This event drew on the experience of MIT and the delivery of their globally recognised Regional Entrepreneurial Acceleration Programme (REAP) which engages communities around the world to strengthen innovation-driven entrepreneurial ecosystems. The delegates in attendance are all closely aligned to cyber innovation in the North West across a range of sectors.

The event also attracted global speakers, keynotes, and panel discussions from industry and innovation

leaders such as Dr Phil Budden (MIT), Andrew Roughan (CEO, Plexal), Professor Simon Cook (Professor in Practice at Lancaster University), Dr Alan Gilchrist (Quantum Base), Gordon Bateman (CEO, CRSI), David Eaves (Westinghouse), Dr Natalie Jones (EPSRC), Professor Mandy Parkinson (Salford Business School), Helen Wilding (GMCA) and Dion Williams (Lancaster University). Collectively, the delegates discussed the cyber ecosystem in the region and best practice in supporting innovation driven enterprises, entrepreneurial ecosystems and promoting growth.

This update paper summarises the key feedback from this event and collates the discussion into a single working paper. It also explores the progress made by partners across the North West cyber ecosystem in recent years, and how the region is performing against the baseline statistics and recommendations set out in the North West Cyber Corridor research.

The ambition of this paper is to ensure that all key partners can work collaboratively in the coming months and years across a range of projects aimed to enhance the ecosystem.

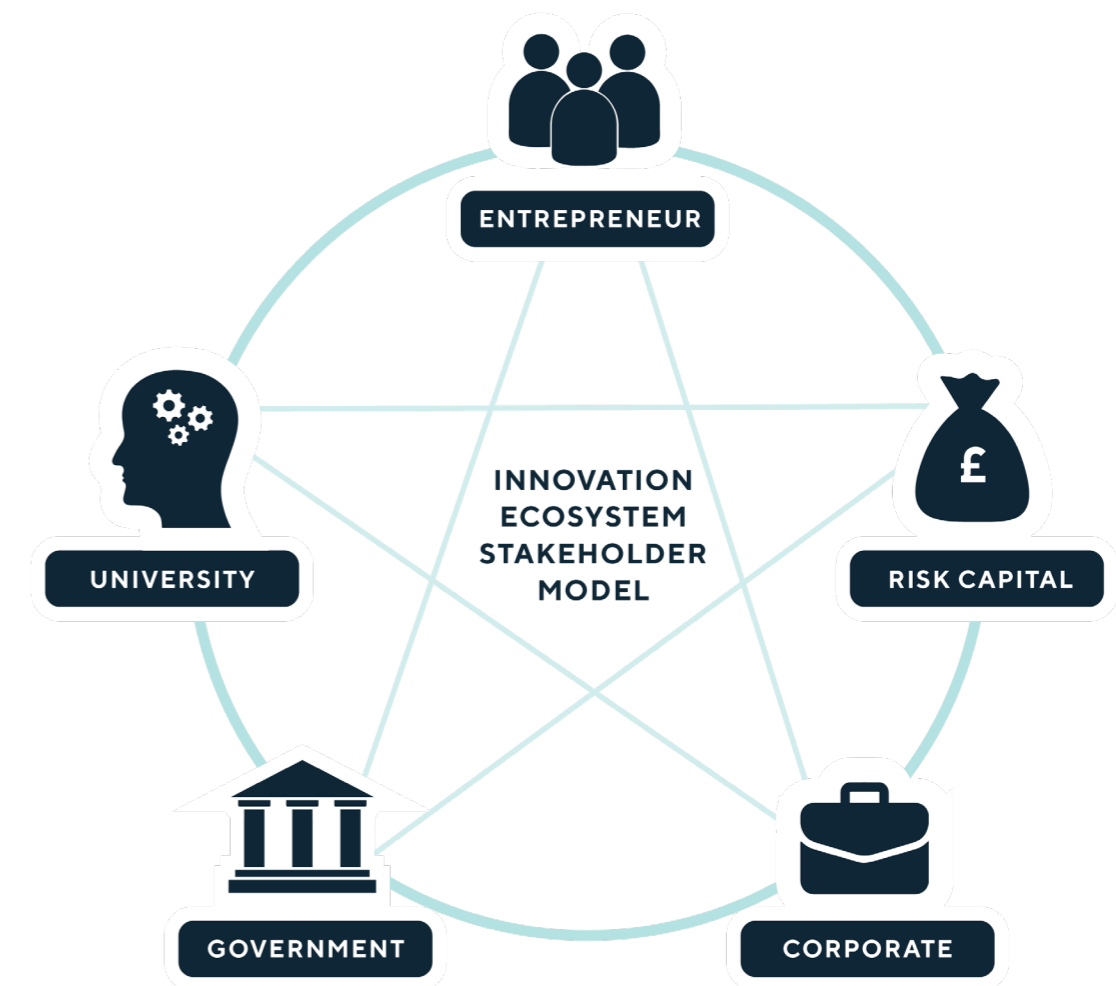
¹ In partnership with University of Manchester, Manchester Metropolitan University, University of Liverpool, University of Salford, and University of Central Lancashire (UCLan), alongside partners from Plexal, CSRI, and Massachusetts Institute

03 MIT REAP Framework & Workshop Summary

The North West has a wide network of stakeholders working together to support a thriving and innovative cyber ecosystem in the region.

Break-out sessions were held to explore the five key players, based on the MIT REAP Stakeholder Model² of Entrepreneurs, Risk Capital (Investment),

Corporate, Government (and civic engagement) and Universities) that can shape the development of the cyber security ecosystem. Each session included key feedback from stakeholders, with a scribe assigned to capture the views.



² Budden, P. & Murray, P. (2019) 'An MIT Approach to Innovation: eco/systems, capacities & stakeholders.' Available at: <https://reap.mit.edu/assets/An-MIT-Approach-to-Innovation.pdf>

04

Core Feedback

The core feedback from the five main stakeholder groups under the MIT REAP model are set out below, as well as their shared insights for developing the ecosystem. Across the event, there was extensive feedback shared across the themes, including:

01 The importance of collaboration and strategic focus:

The North West is home to several world-leading universities, businesses, innovation centres, and policy leads. These can often have a clear geographic remit; however, the discussion recognises the need for collaboration between organisations to maximise inward and external investment and provide clear strategy and support to the ecosystem. The NW CyberCom project is a clear example of this collaborative focus.

02 The need for cohesive partnerships and intermediaries

to bring together innovative ideas and research, encourage high potential start-ups, and enable access to external investment and broker commercial opportunities.

03 The critical role of universities and the wider ecosystem in supporting national security objectives,

particularly driven by the role of the National Cyber Security Centre and GCHQ in Manchester, and the arrival of the National Cyber Force in Sarnesbury.

04 The significance of place-based funding:

Public organisations can shape the narrative and articulate the benefits of supporting the ecosystem. They help to position the cyber corridor with wider stakeholders – signaling what the opportunities and ambitions are and bring people and investment into this vision.

05 The need for inclusivity and vision in developing the skills pipeline for growth:

Growing the cyber ecosystem offers the potential for good jobs, improving resilience, and creating opportunities for the wider community. Developing skills and access to opportunities across the region, and helping young people and communities become involved in cyber security is vital to long-term sustainable and inclusive growth.

CIVIC (GOVERNMENT):

- **Place-Based Funding:**
There is a key role for the public sector to support research and develop narratives to maximise inward investment and place-based funding.
- **Regional Positioning:**
Position the North West cyber corridor as a national asset and leader in the UK's cyber and defence community.
- **Community Engagement:**
Articulate the benefits of the cyber ecosystem to local communities.
- **Ecosystem Support:**
Provide sustained support for the growth of the cyber ecosystem.
- **Infrastructure Planning:**
Develop and implement plans for necessary infrastructure to support the cyber sector.
- **Talent Retention:**
Create strategies to retain spin-out companies and talent within the region.

INVESTORS:

- **Increasing deal flow and opportunities:**
Increase the flow and value of investment within the cyber sector.
- **Developing an investment pipeline:**
Support an increased supply of startups, support commercialisation, and work with accelerators and incubators to develop a pipeline for investment.
- **Broadening investment:**
Work with investors to widen strategies to accommodate longer development cycles in cyber and explore the development of a dedicated cyber-focused investment fund.
- **Cyber Knowledge Gap:**
Regional and national investors can often lack sufficient exposure to cyber security deals to develop specialised knowledge or domain expertise. They typically require a lead investor with deep cyber expertise to lead, help de-risk the investment, and validate the opportunity.
- **Expert Engagement:**
Engage experienced cyber technologists to bring expertise to the ecosystem, and advocate for government backing and support for cyber investment.

CORPORATES:

- **Brand Leverage:**
Leverage the North West brand and Cyber Corridor proposition for competitive advantage.
- **SME Engagement:**
Actively engage with the innovative SME base in the region.
- **Skills Gap Bridging:**
Work with universities to address the skills gap in the cyber sector.
- **Sector Mobility:**
Promote mobility into the cyber sector from other industries (and vice versa to develop a cyber security culture across the region).
- **Innovation Hubs:**
Develop, fund and support innovation sites and centres of excellence for cyber and related technology.
- **R&D Participation:**
Lead regional R&D collaborations to drive innovation (e.g. co-funding research with universities).
- **Community Partnerships:**
Build and maintain strong community partnerships to support the ecosystem and promote inclusion.

ENTREPRENEURS

- **Developing and attracting talent:**
The need for a sustainable regional talent pool, with talent available to academia, start-ups, corporates, and public sector and defence. Implement effective strategies for retaining talent in the region.
- **Bolstering Research & Development:**
Leverage university R&D capabilities for innovation and product development.
- **Brokering partnerships between corporates and start-ups:**
Address and fulfil corporate innovation needs through entrepreneurial ventures.

ENTREPRENEURS (CONT.)

- **Early-Stage Funding:**
Securing high quality early-stage funding for cyber startups.
- **Prime Partnerships:**
Build strategic partnerships with large prime contractors in the cyber sector. Work with partners such as Plexal to maximise innovation spillovers.
- **Government Access:**
Streamline access to government resources, support, and procurement.

UNIVERSITIES:

- **Ecosystem Collaboration:**
Foster and facilitate collaboration within the cyber ecosystem by bringing universities and partners together.
- **Promoting Security and Defence Research:**
Contribute significantly to defence and security research initiatives, aligned to the regional economy.
- **Regional Testbed:**
Develop the North West region as an innovation testbed for cyber technologies.
- **Supporting a Risk-Taking Culture:**
Encourage calculated risk-taking and entrepreneurialism in academic and research environments.
- **Commercialisation Pathways:**
Improve pathways for commercialising academic research in cyber.
- **Flexible Skill Development:**
Implement flexible approaches to skills development and industry engagement.
- **Enterprise Education:**
Develop and promote enterprise-level education in cyber-related fields (e.g. Cyber MBAs and life-long learning).

Developing the North West Cyber Ecosystem: Shared Insights

- Adapt MIT's REAP model locally
- Enhance cyber innovation & entrepreneurship
- Promote cross-sector collaboration
- Strategic investment & leadership
- Focus on sustainable growth

Universities:

- Foster ecosystem collaboration
- Contribute to defence & security research
- Develop the region as innovation testbed
- Streamline academic processes and encourage risk-taking
- Improve commercialisation pathways
- Implement flexible approaches to skills development and industry engagement
- Develop enterprise level education

Civic:

- Develop place-based funding narratives
- Complement research strengths
- Position cyber corridor nationally
- Articulate community benefits
- Support ecosystem growth
- Plan infrastructure development
- Retain spin-outs in region

Entrepreneurs:

- Tap into regional talent pool
- Leverage university R&D capabilities
- Address corporate innovation needs
- Implement talent retention strategies
- Secure early-stage funding
- Build partnerships with large primes
- Streamline access to government
- Improve access to capital

Investors:

- Increase deal flow in cyber sector
- Improve pitch clarity and transparency
- Adjust for longer development cycles
- Support commercialisation processes
- Address IP protection challenges
- Create cyber-focused investment fund
- Engage experienced cyber investors
- Advocate for government backing

Corporates:

- Leverage the brand & Cyber Corridor proposition
- Engage with innovative SME base
- Address skills gap with universities
- Promote sector mobility (into cyber)
- Develop innovation sites and centers of excellence
- Lead regional R&D collaborations
- Build community partnership

05

Sustaining the Momentum

The North West Cyber Corridor baseline research highlights the potential for the cyber security ecosystem, which can be catalysed from an existing strong base. The North West continues to be the largest UK cluster for cyber security (outside of London and the South East), with over 10% of the national cyber security workforce³.

There are some particularly encouraging signals that partners are continuing to enhance the ecosystem across industry, infrastructure, skills, and investment. We set out some of the key growth signals over the last twelve months, that partners should build upon to sustain the momentum – and help the ecosystem achieve 30,000 FTEs by 2035.

 **350**

Number of cyber security businesses

 **55%**

Of H1 2024 cyber security investment in the North West

 **30,000**

Target for FTEs by 2035

³ DSIT (2024) Cyber security sectoral analysis 2024 <https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2024/cyber-security-sectoral-analysis-2024#regional-snapshots>

INDUSTRY

An increasing number of cyber security start-ups in the region:

The baseline report identified c. three hundred cyber security businesses in the region in 2022/23. Current research (ongoing as part of the DSIT 2025 Cyber Security Sectoral Analysis) suggests this figure is now closer to 350 businesses, suggesting an increase in start-ups, and businesses establishing offices in the North West. Lancaster University shall continue to track this measure with Perspective Economics.

An increased recognition for the region's cyber security industry

The region has been active in hosting a range of cyber security conferences and initiatives (e.g., Lancashire Cyber Festival, the Lancaster Cyber Leadership Symposium, The Future of Cyber Security Manchester etc.), and Manchester will host CyberUK in 2025. Regional SMEs have also taken part in schemes such as Cyber Runway and NCSC for Startups. In June 2024, Lancaster University spinout company Mindgard won the award for the 'UK's Most Innovative Cyber SME 2024' at Infosecurity Europe 2024, after raising £3m in Sept 2023.

Increased investment for the region's cyber security industry

Previous DSIT Cyber Security Sectoral Analyses have highlighted how the North West has been the third largest region for cyber security related VC investment in the UK in recent years. However, this is within a context of regional imbalance of investment across the UK and sectors, and the research has recommended a sustained push to increase deal flow and investment across the regions.

It is encouraging that the in the last four quarters (July 2023 – June 2024), according to Perspective Economics analysis of Beauhurst investment data – the North West has been home to the largest VC investment in UK cyber security this year, with Cheshire-based PortSwigger securing £88m in first external investment to accelerate its international footprint. This is a significant deal, and PortSwigger has bootstrapped and self-funded to this point – highlighting the expansionary potential in the region. Further, Manchester based CultureAI (a human risk monitoring platform) raised £8m in a Series A investment in July 2024. ESProfiler has also raised £2.8m at seed stage, and has benefitted from its partnerships with DISHmcr, NCSC for Startups and Plexal. Lancaster University spin-out Mindgard also secured a £3m seed investment in 2023.

Overall, this means that 55% of the investment raised in the UK cyber ecosystem in the first half of 2024 has been in the North West.

INFRASTRUCTURE

Innovation-led infrastructure embedding in the region

The baseline report highlighted over twenty high quality coworking and incubation spaces with a digital and cyber security focus, including Digital Innovation Security Hub (DiSH) at Heron House, Fraser House, and InfoLab21 in Lancaster, and several Bruntwood SciTech sites. Lancaster University has also recently opened the Lancaster Environment for New Security (LENS) and Decision Theatre in 2024, as it further developed its co-location, collaboration and training facilities.

In the past twelve months, these spaces have contributed significantly to the development of the start-up and cyber ecosystem across the North West – as reflected through increased partnerships and investment.

SKILLS & TALENT

Advancing the skills and research pipeline

There have been several welcome skills and education initiatives advanced by the region's universities in recent months, including:

- The significant NW CyberCom project, funded by Research England, bringing six partner universities together with industry and innovation partners for the first time.
- Lancaster University's £19m investment in its data and cyber security research, teaching and innovation capabilities to support the National Cyber Force and the development of the North West Cyber Corridor.
- University of Manchester's £4.7 million investment in AI and trust capability to enhance research and teaching.
- UCLan's announcement of additional funding for new degree apprenticeships in cyber security and engineering
- Lancaster University and IN4 Group programme to develop tech talent through establishment of 24 CyberFirst Gold Hubs, one in each of the North West Local Authority areas.
- BAE Systems sponsoring the 40 new cyber professionals via the Capslock Certified Cyber Security Practitioner course with fully funded places provided by the UK Government's Skills Bootcamp
- Lancaster University offering the only Cyber MBA programme with provisional certification from the National Cyber Security Centre.

However, there are several ongoing global challenges that partners must continue to consider and address at a regional level. For example:

- There is a challenging labour market within wider tech, and for entry-level talent, particularly driven by macroeconomic trends and tech sector efficiencies. The number of cyber security job postings is estimated to have fallen by over 30% in the UK between 2022 – 2023. This makes working with industry and the public sector even more critical to help ensure a long-term skills pipeline beyond education.
- There is a competitive global marketplace for securing inward investment, and many firms are also integrating generative AI approaches into cyber security products and services. This means the North West region must continue to advance and embed its specialisms and relevancy in a national and global setting – at the forefront of securing the UK and diffusing secure digitalisation across several sectors.
- The wider cyber threat landscape remains significant. Many partners within the ecosystem have also experienced and spoken about their own experiences with cyber security breaches. It is essential to take the learning, and work with partners to ensure wider security and resilience across the North West.

06

Developing the North West Cyber Ecosystem

2018

Lancaster University, Manchester Met, University of Manchester, and University of Salford collaborate on the £6m Cyber Foundry project to help protect regional businesses.

2019

GCHQ opens a hub in Manchester, at Heron House, setting up collaborations with local high-tech startup companies

Lancaster University is designated University Enterprise Zone status from Research England in Secure Digitalisation.

2020

Building on the success of GM Cyber Foundry, the £2.1 million Lancashire Cyber Foundry launches to support regional SMEs

2021

The North West Cyber Security Cluster (NWCSC) relaunches, and has since hosted over 30 events and talks

UKG announced the Integrated Review, committing to the development of the North West Cyber Corridor

North West Partnership for Security and Trust launched with Lancaster University, University of Manchester, Manchester Met, University of Salford & GCHQ

National Cyber Force announce plans to build HQ in Samlesbury, bringing over 3,000 jobs to the North West

2022

The DiSHmcr (Digital Security Innovation Hub) opens - a £10m cyber innovation centre, which is co-located at Heron House with GCHQ, led by Barclays Eagle Labs, Plexal, Lancaster University and the University of Manchester

Launch of Lancashire Cyber Alliance to maximise the opportunities from the Cyber Corridor

Lancaster University reveals 'once-in-a-generation investment' in data, cyber security and protection science (with over £19m and 60 jobs)

Lancaster University announces new multi-million pound teaching facilities to educate next generation of computer science and cyber security students

2023

Lancaster University launch the first Executive Cyber MBA and University Academy 92 (UA92) launches a BSc in Cyber Security

Launch of North West Cyber Security Connect for Commercialisation (NW CyberCom)

Netacea, a Manchester-based cyber security business, secures a £4.4m investment to support continued growth

Lancashire Cyber Festival & Lancashire Cyber Partnership announced

GMCA launch the Greater Manchester Cyber Strategy 2023-2028

Lancaster University and Plexal publish the North West Cyber Corridor Impact Study

2024

Lancaster University and IN4 Group sign contract to develop tech talent through establishment of 24 CyberFirst Gold Hubs, one in each of the North West Local Authority areas

MIT joins the NW CyberCom to support identity opportunities to grow the North West cyber ecosystem

University of Manchester announce a £4.7 million investment in AI and trust capability to enhance research and teaching in humanities

UCLan announce funding for new degree apprenticeships in cyber security and engineering

FHundED Live, Lancashire's new digital industries conference, brings over 100 business leaders together in Lancaster

Lancaster University spinout company Mindgard wins 'UK's Most Innovative Cyber SME 2024' award at Infosecurity Europe 2024.

Cheshire-based PortSwigger secures £88m in first external investment, Manchester-based CultureAI raises £8m to support 'break-out growth', and Manchester-based ESProfiler raises £2.8m million to help enterprises maximise their ROI on security investment

Lancaster invests **£1m** from the Regional Innovation Fund to develop a vibrant co-working and collaboration space for cyber security related businesses and government organisations known as Lancaster Environment for New Security (LENS), and develops a new Decision Theatre and Digital Training Labs **supported by a £4m grant from the Office for Students (OfS)**

2025

The National Cyber Force will establish its HQ in Samlesbury, bringing over 3,000 jobs and new growth for the region's cyber ecosystem



