QUEEN'S UNIVERSITY BELFAST | CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

perspective economics

DECEMBER 2025

Northern Ireland Cyber Security Snapshot

2025 Update

CONTENTS

EXECUTIVE SUMMARY

The Centre of Secure Information Technologies (CSIT) is the UK's Innovation and Knowledge Centre (IKC) for cyber security, delivered in collaboration with Innovate UK, the Engineering and Physical Sciences Research Council (EPSRC) and Invest Northern Ireland (Invest NI). CSIT is committed to world class research and accelerating translation activity for economic impact. The centre also works collaboratively with the National Cyber Security Centre (NCSC), ensuring that the UK is the safest place to live and work online.

In February 2023, CSIT secured an £18.9m investment in the region's cyber security ecosystem, including £11 million of UK Government funding through the New Deal for Northern Ireland (NI), to help develop a pipeline of cyber security professionals in NI and provide collaborative research and development opportunities with industry through the creation of a Cyber-AI Hub (CAI Hub). The CAI Hub is also supported by £3.3m of funding from the EPSRC, to deliver the third phase of CSIT's IKC programme, focused on "Securing Complex Systems", cementing the Centre's position as a world-leading centre for research and innovation until 2027.

This document is the fourth in a series of short overviews of the Northern Ireland cyber security ecosystem. It shows that Northern Ireland continues to be an international hotspot for cyber security activity. Local companies offer a full spectrum of cyber security products and services, and Northern Ireland's ecosystem supports cyber security technology development across all technology readiness levels.

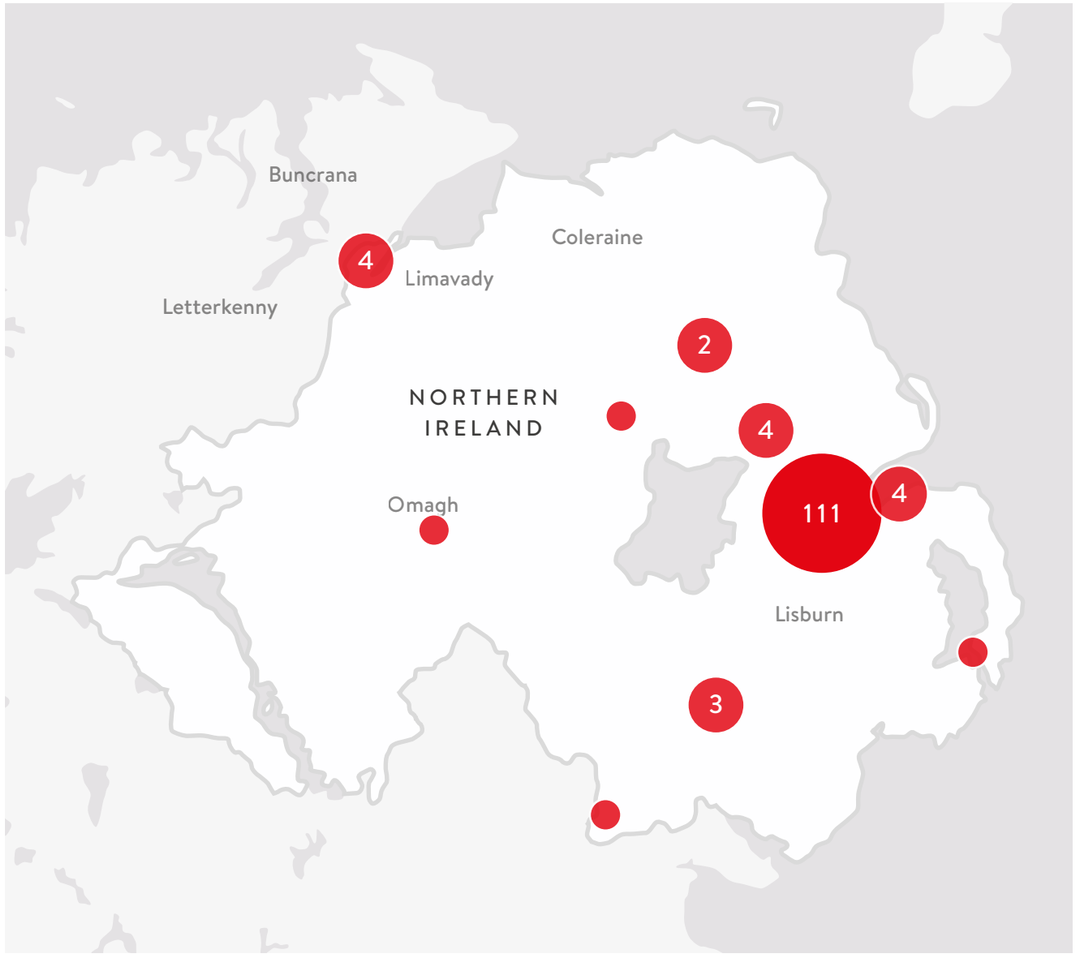
Cyber security continues to be one of the region's economic success stories, with over 2,750 related roles generating more than £258m direct GVA to the economy. However, this research indicates that macroeconomic conditions and technological shifts may impact the trajectory of the ecosystem with respect to employment levels. We note a current backdrop of reduced recruitment activity, inward investment, and growth capital, which is expected to mean that Northern Ireland's target of 5,000 jobs in cyber security may be challenging to meet by 2030.

Despite these challenges, there is an underlying depth in expertise, research activity, and new commercial domains in cyber security that Northern Ireland can best exploit. As such, this report provides an assessment of core challenges and opportunities in the years ahead, to ensure that Northern Ireland's ecosystem is supported to grow and maintain high value added within the region's economy. This will require sustained investment in areas such as research and innovation, updating the positioning and offering of the ecosystem on the global stage, and working collaboratively with public and private stakeholders from across all sectors and domains.

NORTHERN IRELAND'S CYBER ECOSYSTEM

Cyber security is one of Northern Ireland's (NI's) most notable economic success stories, providing an estimated 2,778 jobs and generating over £258m in direct Gross Value Added (GVA) to the local economy. Belfast continues to be one of the world's most concentrated cyber security clusters, with more than one hundred cyber security businesses and teams within three miles of the city centre (Figure I.1).

FIGURE I.1 – LOCATION OF CYBER SECURITY BUSINESSES ACROSS NORTHERN IRELAND



Source: Perspective Economics

Northern Ireland continues to be a leading destination for sustained US cyber security FDI[1], which supports almost 1,800 local cyber security jobs. It has successfully attracted inward investment from around the world, including from Canada, Europe, Japan, the Netherlands, and the Nordics. Overall, two thirds of NI's cyber security firms are headquartered overseas and one third are locally founded.

[1] FDI Markets, 2024

Northern Ireland continues to grow its global cyber security reputation through:

- Its role as an international hub for cyber security research and innovation, underpinned by CSIT.
- An attractive location for inward investment, with partnerships between academia, government, and industry – and access to talent across Belfast, Derry-Londonderry and beyond.
- A growing ecosystem of locally headquartered firms with global reach, supported by leading cluster network 'NI Cyber.'

140
Cyber Security Providers

£258m
Direct GVA to the NI economy

2,778
Employees (2025)

53,300
Average advertised salary 2024

Example Firms:

Signifyd · MetaCompliance · AuditComply · Outsource Group

RapidFort · cloudsmith · Black Duck · Microsoft · kainos

imperva · Anomali · BlackFog · SilverSky · proofpoint

Angoka · NVIDIA · Kigen · Salt Secure Communications · Cybit · instil

1. INTRODUCTION

This report provides an update to the Centre for Secure Information Technologies (CSIT) Northern Ireland Cyber Security Snapshot 2024 and includes an overview of the cyber security market in Northern Ireland up to October 2025 spanning key products and services, financial performance, investment, research and innovation, and labour market activity.

1.1. BACKGROUND & CONTEXT

The Centre of Secure Information Technologies (CSIT) is the UK's Innovation and Knowledge Centre (IKC) for cyber security, delivered in collaboration with Innovate UK, the Engineering and Physical Sciences Research Council (EPSRC) and Invest Northern Ireland.

In February 2023, CSIT secured an £18.9m investment in the region's cyber security ecosystem. This included £11m in UK Government funding through the New Deal for Northern Ireland, which is being used by CSIT to further develop the pipeline of talent within the region and to provide collaborative research and development opportunities with industry through the creation of a Cyber-AI Hub. Further support to CSIT has been provided by EPSRC, including £3.3m of funding which will be used to deliver the third phase of CSIT's IKC programme. This work is focused on 'Securing Complex Systems' and will support CSIT activities until 2027.

Perspective Economics has been commissioned by CSIT to undertake an annual Cyber Security Sector Snapshot (2023 – 2025), with additional market intelligence support to enable further strategic and monitoring and evaluation activities. Specifically, the analyses in this report are intended to support CSIT in tracking developments within the cyber security sector in Northern Ireland.

1.2. RESEARCH SCOPE & DEFINITION

The cyber security sector does not have a formal Standard Industrial Classification (SIC) code. The research team have therefore worked closely with CSIT to develop a sector definition and taxonomy that reflects the unique cyber security offering within Northern Ireland, but is also closely aligned to national strategy, and previous research conducted on behalf of the Department for Science, Innovation and Technology (DSIT). In the context of this study, cyber security is defined as:

> "The protection of internet connected systems (to include hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm, or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so."
>
> - UK National Cyber Security Strategy

Table 1.1 provides an overview of the taxonomy adopted by the research team to identify cyber security businesses in Northern Ireland. These classifications have been developed to reflect relevant to the specialisms offered by firms operating in the sector specific to Northern Ireland, acknowledging the region's particular strength in securing inward investment, and the establishment of several high-value Research and Development (R&D) offices and Security Operation Centres (SOCs).

TABLE 1.1 – SECTOR TAXONOMY CLASSIFICATION

Sector Specialism	Definitions
Identification, Authentication and Access Control	Systems designed to support the verification of users accessing systems e.g. Salt Communications
Risk, Compliance and Fraud	Solutions to identify risks (such as harmful actors or anomalies), ensuring compliance with cyber security standards e.g. MetaCompliance, Signifyd
Securing Applications, Networks and Cloud	Customisable solutions for identifying and patching potential software or network exploits or applying secure parameters to network or cloud e.g. Black Duck, Contrast Security
Threat Intelligence, Monitoring, Detection and Analysis	Information security professional services focusing on network administration or network engineering that helps counter the activities of cyber criminals such as hackers and developers of malicious software e.g. Rapd7, Proofpoint
Operational Technology (OT) Security and Connected Devices	Manufacturing and distribution of programmable systems or devices that interact with the physical environment (or managed devices that interact with the physical environment) e.g. Kigen, Wolfspeed
Managed Security Service Provision (MSSPs) and Advisory Services	Outsourced cyber security solutions focused on monitoring, network security, patching and remote device management, penetration testing, and wider security and IT advice e.g. Capita, Agio, LoughTec

Source: Perspective Economics, CSIT

2. CYBER SECURITY IN NORTHERN IRELAND

Northern Ireland continues to be a globally recognised cyber security ecosystem, with a wide range of positive feedback and acclaim from companies, investors, academia, and government. Previous snapshot reports have highlighted how the Northern Ireland cyber security ecosystem has evolved over the last two decades, from a small number of businesses employing a few hundred people to over 140 businesses with almost three thousand people employed.

This section updates the evidence base underpinning Northern Ireland's strength and opportunity within its cyber security industry. It explores the number of cyber security businesses in Northern Ireland, including what they offer, their location, and classification by size, type, and industry focus. This report also recognises that there are significant structural and macroeconomic factors shaping the cyber security ecosystem, both in Northern Ireland, across the UK and globally. These factors, such as downward pressure on global Foreign Direct Investment, the increased deployment of automation and AI, merger and acquisition activity among parent firms, and a broader emphasis upon workforce efficiency may all lead to a more defensive rather than expansionary labour market.

This updated report therefore provides a more critical assessment of the current size, scale, structure, and potential interventions to support growth in the NI cyber security ecosystem to 2030.

2.1. ECOSYSTEM DEVELOPMENT TIMELINE

As set out within previous reports, the growth of Northern Ireland's cyber security sector is not a sudden phenomenon, nor overnight success. It is, rather, the result of consistent effort and sustained investment, over the last twenty-five years (Figure 2.1).

FIGURE 2.1 – NI CYBER SECURITY ECOSYSTEM DEVELOPMENT TIMELINE

1998
Belfast (Good Friday Agreement).

1999
Northern Ireland Science Park (now Catalyst) set-up in Titanic Quarter.

Allstate Northern Ireland founded.

2003
MetaCompliance founded.

2004
Mail Distiller founded (email security).

Queens University Belfast Institute of Electronics, Communications & Information Technology (ECIT) founded in Titanic Quarter.

2006
Mail Distiller founded (email security).

2007
Skurio, ANSEC IA founded.

2008
ECIT hosts the UK's Innovation and Knowledge Centre (IKC) for Cyber security, the Centre for Secure Information Technologies (CSIT) - opened 2009. IBM (Security) sets up presence Titanic Quarter.

2011
CSIT one of the first six Academic Centres of Excellence in Cyber Security Research recognised by GCHQ.

2012
SaltDNA founded. .

2013
Mail Distiller acquired by Proofpoint. Belfast secures an IBM Smarter Cities Challange Grant.

2014
Emergence of NI's domestic cyber security sector: Ampliphae, B-Secur, Cyphra (now Cybit), AuditComply founded.

CSIT sets up one of the first MSc in Applied Cyber Security, which has enrolled hundreds of students since starting. Rapid7 establishes offices in NI.

2015
Liopa founded (commercialising over 15 years of research at QUB in speech and image processing).

CSIT awarded The Queen's Anniversary Prize for its work in strengthening global cyber security and protecting billions of internet users around the world and for its economic impact.

2016
Black Duck establish Belfast office.

2017
CSIT hosts AppSec. Anomali creates 120 jobs.

2018
CSIT partners with cyber innovation centre LORCA. Aflac, Signifyd, Imperva, NI Cyber (cluster) set up. CSIT hosts NI's first CyberFirst event for schools.

NI confirmed as the top international investment destination for US sourced FDI cyber projects.

2019
Contrast Security announces 120 jobs.

Angoka founded.

2020
Microsoft opens 85 person cyber security centre.

Cygilant (now SilverSky) establishes a global SOC in Belfast (65 jobs).

Titan IC acquired by Mellanox, then Nvidia.

2021
Rapid7 opens new office in central Belfast with room for 400 employees, and is Rapid7's largest engineering hub globally.

KPMG runs Cyber Security Assured Skills Academy with DfE.

Telefonica Tech expands its Belfast SOC.

Agio, Nihon Cyber and Nisos announce NI offices.

CSIT partners with the Royal Air Force on pioneering innovation node for NI to develop the cyber related defence supply chain in the region.

2022
BT opens state-of-the-art Security Operations Centre in Belfast, following £6.3m DoF SIEM and SOC managed services award.

Outsource Group and Ansec IA merge to create an NI security 'powerhouse'.

CSIT awarded £3.3m by EPSRC for delivering the next Phase of the IKC, and becomes only the third university to join the Rolls-Royce Global CyberTechnology Research Network.

2023
UK Government announces £18.9m investment in CSIT's Cyber-AI Hub.

Belfast hosts CyberUK.

Cloudsmith secures one of the largest investments in an NI tech start-up to date.

2024
BlackFog selects Belfast as its UK R&D HQ.

2025
MetaCompliance secures investment from Keensight Capital.

Vertical Structure acquired by Instil.

Ampliphae acquired by Arqit.

Angoka invests £1.8m in manufacturing cyber security with AMIC and Invest NI.

CSIT supports launch of LASR, and continues to deliver Cyber-AI Hub initiative.

2.2. KEY UPDATES IN THE NICYBER SECURITY ECOSYSTEM (2024-2025)

Over the past twelve months, there have been several announcements and initiatives which have and will shape the NI cyber security ecosystem. These span several strategic domains, including private investments, exits and acquisitions, new funding for academic research, support for commercial research and development activity, and investment in skills development. In tandem, the Centre for Secure Information Technologies (CSIT) has also increased its efforts to successfully embed AI security within the region through the Cyber-AI Hub, as well as increase research and partnership activity in areas such as cryptography, post quantum encryption (PQE), connected devices and hardware, 6G networks, and industrial control systems.

Whilst this report highlights a 'slowing' of cyber security recruitment activity, there have been several high-value strategic announcements for the NI ecosystem that could significantly support broadened growth in the years ahead. We summarise some of these updates below:

- **UK-US Investment:** In September 2025, Bank of America announced that is set to establish a Belfast office, creating up to 1,000 new jobs, though further detail is still to emerge on the profile of the roles. Further, Citi also confirmed an investment of £1.1bn across its UK operations including Belfast. Whilst these are aligned to financial services, it is anticipated several of these roles will include a focus on governance, risk, and compliance roles (GRC) as well as functions highly aligned to cyber security and defence. This investment will also create a new 'anchor' tenant for the local ecosystem providing greater resilience and opportunities within the labour market.

- **MetaCompliance:** In late 2024, Derry/Londonderry-based MetaCompliance, a leader in human risk and cyber security awareness, secured investment from Keensight Capital, a leading European private equity firm. Over the last three years, it has 'more than doubled its headcount to over two hundred employees' serving customers across the UK, Europe and beyond. At the time of writing, it has several open positions in Derry/Londonderry, in addition to expanding in Marseille, Leipzig, and Porto. This investment demonstrates a moment of maturity for the local cyber security ecosystem, where a company founded and scaled in the North West has attracted investment from a leading European private equity firm, and continues to scale globally.

- **Instil and Vertical Structure:** The acquisition of Vertical Structure (a specialist cyber security consultancy) by Instil (a leading software engineering firm) also marks notable maturity and strategic activity in the local ecosystem. This acquisition will enable Instil to offer 'secure-by-design' software development services and aligns strongly with increased commercial and policy focus on software security. Instil has also announced its plans to increase turnover three-fold by 2028, and invest over £6m in its growth strategy supporting over 100 new high-value jobs with support from Invest NI.

- **Ampliphae acquired by Arqit:** In May 2025, Arqit, a leader in quantum-safe encryption, announced the acquisition of Ampliphae's product portfolio IP and innovations team. Ampliphae's encryption risk advisory service will be available to enterprises and governments worldwide.

- **Angoka:** In June 2025, ANGOKA announced its investment of £1.8m in a COSMIC (Cybersecurity for Operational Systems in Manufacturing and Industrial Control) initiative, in partnership with the Advanced Manufacturing Innovation Centre (AMIC) and support from Invest NI. This will support protecting manufacturing firms from cyber threats that can impact the operational resilience of equipment and processing.

- **An increased focus on AI Security:** The ongoing investment in CSIT's Cyber-AI Hub has enabled further partnerships with firms such as NVIDIA and Rapid7, focusing on AI and cloud security. Further, CSIT has supported the launch of the UK Government backed Laboratory for AI Security Research (LASR) with Plexal, Alan Turing Institute, University of Oxford, FCDO and DSIT – with local firms such as Pytilia taking part in the LASR Validate programme. Further, the Artificial Intelligence Collaboration Centre (AICC) is well underway delivered by UU and QUB, with CSIT's Cyber-AI Hub Director on the board. The recent AI Capability Census also notes the opportunities for Northern Ireland to become a hotbed for ethical AI development – with a **'strong emphasis on compliance, governance, and security within AI services which reflects a pragmatic understanding of enterprise concerns about AI adoption risks, and the need to embed solutions securely and fairly. For example, Kainos recently led on creating the DSIT Code of Practice for AI Cyber Security.'**

- **Investment in Skills:** In November 2024, PEACEPLUS funding was awarded to the North West Digital Employment Pathway Training Hub (NW DEPTH) initiative. This will run for four years in Donegal and Derry City and Strabane and see c. €10m in investment in digital skills in the North West. It is anticipated this will support over 2,000 participants to gain access to employment-focused digital and cyber security education programmes free of charge.

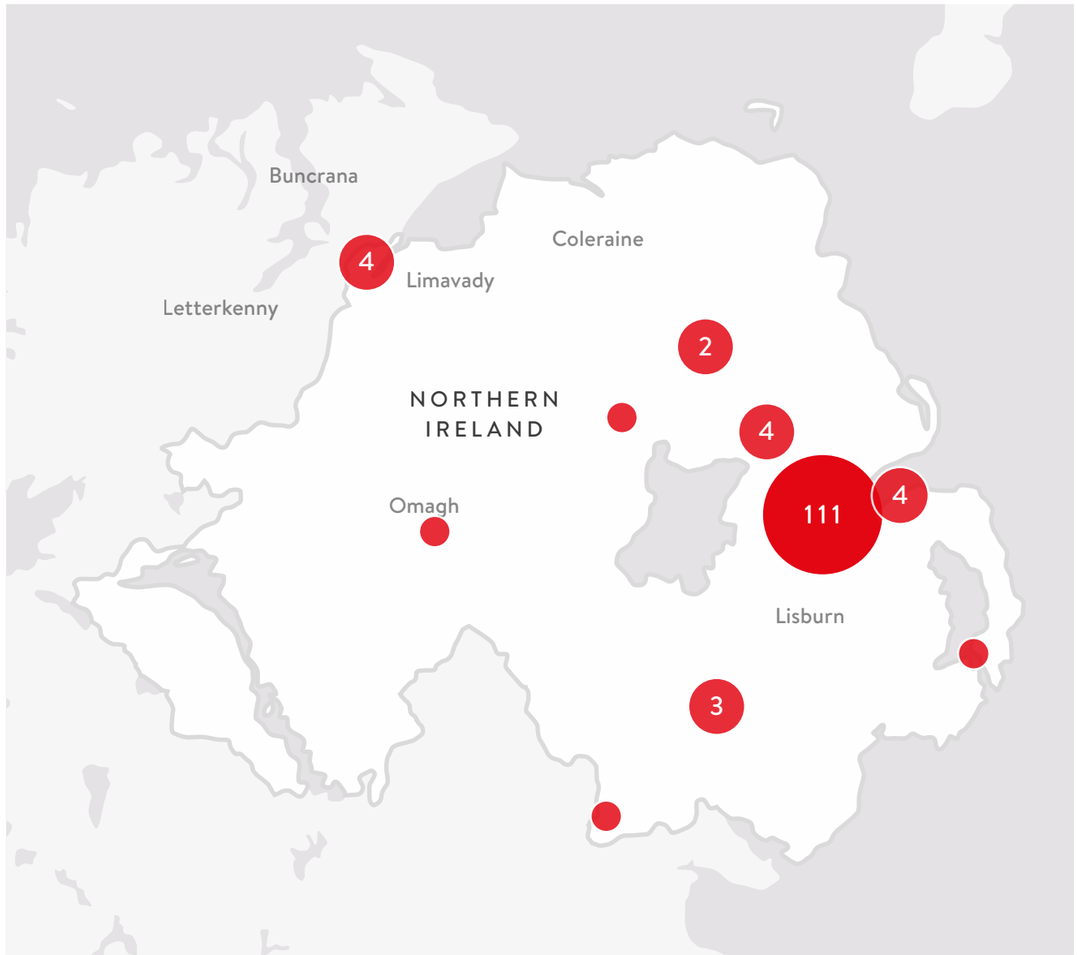
2.3. NUMBER AND TYPE OF CYBER SECURITY FIRMS

The research team has identified **140 companies (an increase from 128 in the 2024 report) in Northern Ireland that either provide a cyber security product or service to market or are actively employing a cyber security team** in Northern Ireland that contributes to a commercial outcome (e.g. an insurance firm with a dedicated cyber security operation in Northern Ireland). The methodology used to identify cyber security businesses and employees operating within Northern Ireland is consistent with the UK Cyber Security Sectoral Analysis 2025 research undertaken for DSIT.

2.4. GEOGRAPHIC DISTRIBUTION

Belfast continues to be one of the world's most concentrated cyber security clusters, with more than one hundred cyber security businesses and teams within three miles of the city centre (Figure 2.2). Belfast is home to 84% of Northern Ireland cyber security firms, however, there are also opportunities to build and scale teams within the North West region where firms such as MetaCompliance have shown significant growth in recent years, as well as areas such as Lisburn and Castlereagh, and Antrim, where increasingly firms with a strong IT managed services presence are increasingly adopting credentials and capabilities to provide clients with schemes such as Cyber Essentials or provide NCSC Cyber Advisor status to SMEs.

FIGURE 2.2 – LOCATION OF NI CYBER BUSINESSES



Source: Perspective Economics

2.5. CYBER SECURITY CAPABILITIES

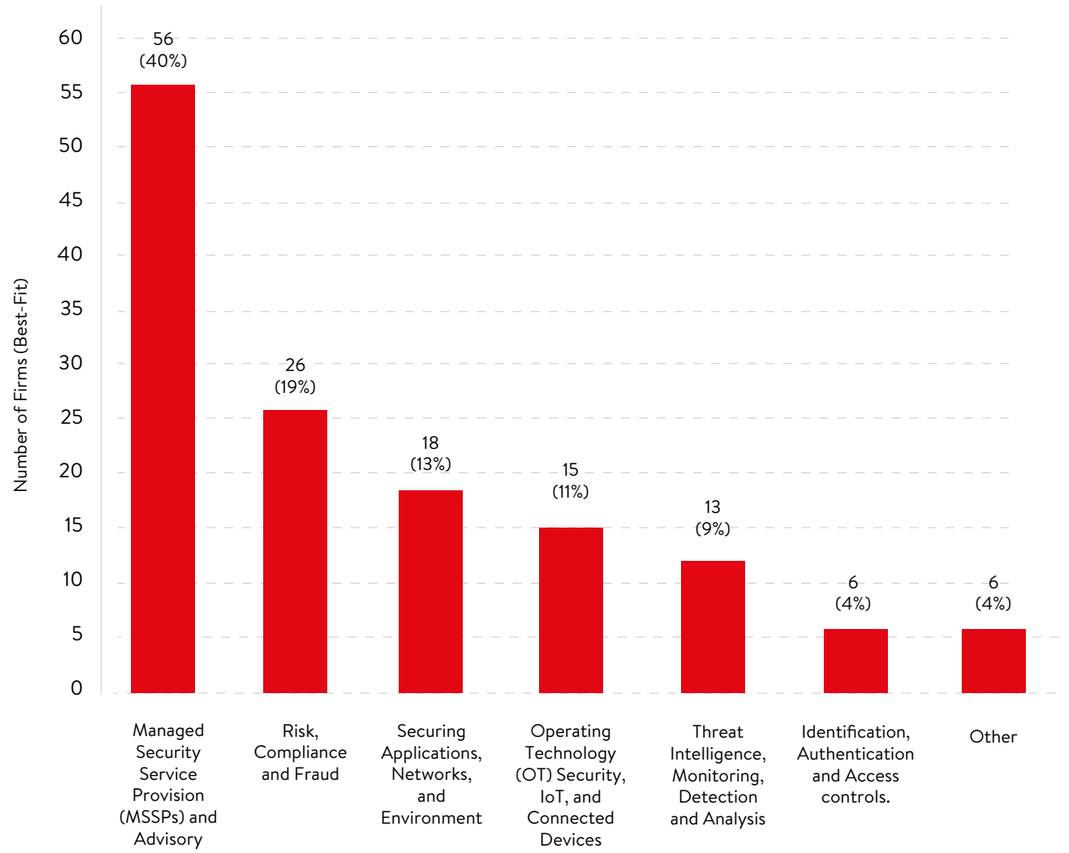
We estimate that 32 percent of Northern Ireland's cyber security firms are dedicated firms i.e., cyber security products and services represent the core of their business offer (n=45). This in-crease has been driven by a small number of newly registered cyber security advisory firms in the last twelve months. A further 68 percent of firms are diversified, meaning that cyber security products and services represent one part of a broader business offer (n=95).

To further understand the capabilities of the cyber security sector in Northern Ireland the study team has compiled descriptive information regarding the products and services offered by each of the 140 cyber security firms. Data is compiled from both web-based and proprietary data sources and is used to align core capabilities to the taxonomy presented in Table 1.1.

Figure 2.3 uses a 'best-fit' classification to illustrate the core capabilities of cyber security firms in Northern Ireland, highlighting strengths in the following areas:

- Managed Security Service Provision and Advisory Services.
- Risk, Compliance and Fraud.
- Securing Applications, Networks and Cloud.
- Operating Technology (OT) Security and Connected Devices.
- Threat Intelligence, Monitoring, Detection and Analysis.
- Identification, Authentication and Access Control.

FIGURE 2.3 – CORE CAPABILITIES WITHIN NORTHERN IRELAND'S CYBER SECURITY ECOSYSTEM



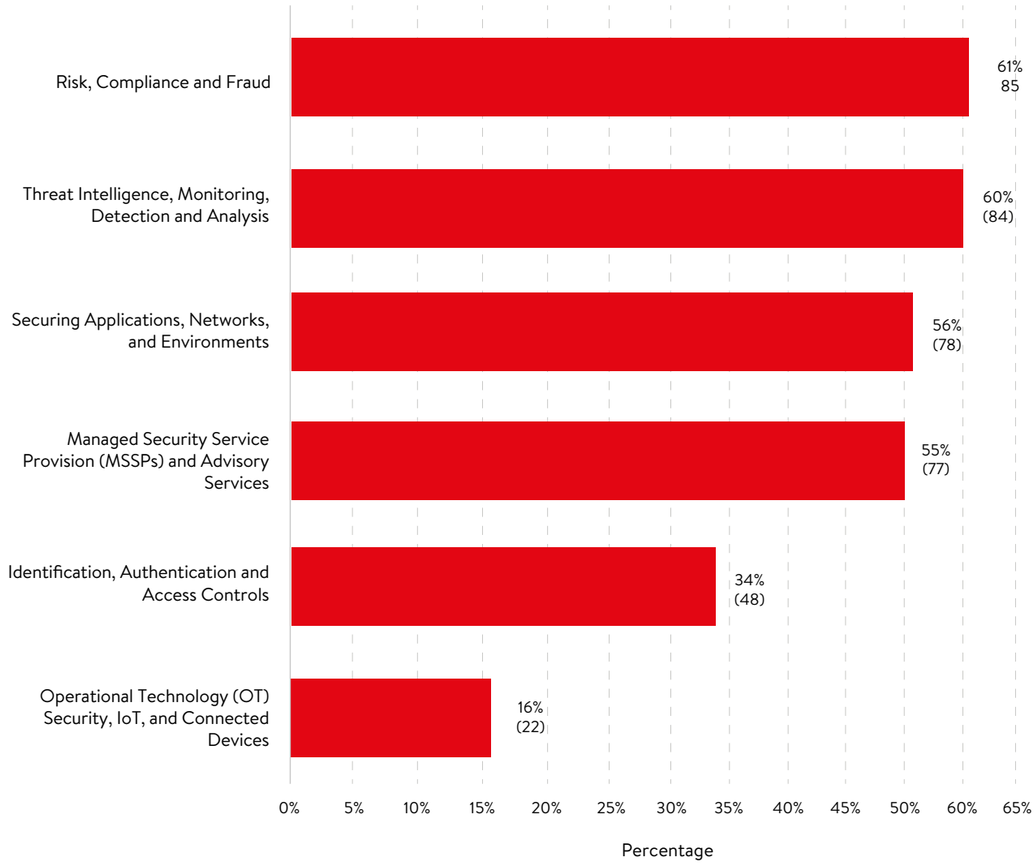
Source: Perspective Economics, CSIT

Overall, the 2025 best-fit classification shows consistency in core capabilities over time, with MSSPs and advisory firms continuing to make up the single most prominent capability again this year. The share of firms with other capabilities also remains broadly consistent with the 2024 study.

To provide a more granular understanding of wider firm capabilities, descriptive information was used to tag each company against each sector taxonomy classification where evidence of corresponding product or service provision was identified.

A total of 394 tags are applied against the 140 firms in the 2025 dataset, meaning that, on average, each company provides products and / or services within two or three of the taxonomy segments. Analysis of these broader tags show diverse capabilities across the NI cyber security ecosystem and highlights the percentage of firms with active capabilities in each of these areas based on web review of product and service provision in cyber security.

FIGURE 2.4 – WIDER FIRM CAPABILITIES



Source: Perspective Economics, CSIT

3. EMPLOYMENT & SKILLS

As of October 2025, there are an estimated 2,778 employees working within Northern Ireland's cyber security sector. This includes all employment within 'dedicated firms' and cyber security related roles only in diversified firms, using review of accounts, web data, and consultation with site leads. This represents a marginal increase of c. 1% since the previous 2024 report (2,754 FTEs), within the context of a challenging macroeconomic environment.

However, it is important to note that this slowdown in the estimated cyber security workforce size reflects a global trend. For example:

- The ISC2 estimates that the **global cyber security workforce in 2024** consists of approximately 5.5m people – reflecting a 0.1% increase since 2023. This compares to a workforce increase of 8.7% between 2022 and 2023.

- This workforce study also reports a 0.7% reduction in the European cyber security workforce, and 2.7% reduction in the North American workforce.

ISC2 also released an updated Workforce Study in 2025, which reports that the cyber security workforce appears to be 'levelling out' rather than continue to decline in 2025. This research highlights that 24% of cyber security teams reported layoffs globally in 2025, compared to 25% in 2025. However, teams reporting hiring freezes has risen from 32% in 2024 to 39% in 2025, and freezes on promotions have also increased from 26% in 2024 to 34% in 2025.[2]

In relation to Northern Ireland's cyber security ecosystem, we estimate that the majority of roles (n= 1759, 63%) are based within firms headquartered within the United States. This means that global trade and investment determinations can directly impact the local cyber security headcount. In recent years, the expansionary climate has resulted in several leading US cyber security firms establishing and increasing headcount within Northern Ireland, which in turn has supported rapid growth in the local ecosystem. However, in the last year, several multinational firms have moved towards increased efficiency with a range of redundancy rounds typically involving between 5 – 15% of workforces globally.

Whilst data is limited upon local impact, particularly where firms announce global layoffs which may impact particular teams more than others, or undertake 'silent' headcount reduction, the longitudinal data available to this study suggests this has had the effect of stalled headcount growth within the sector.

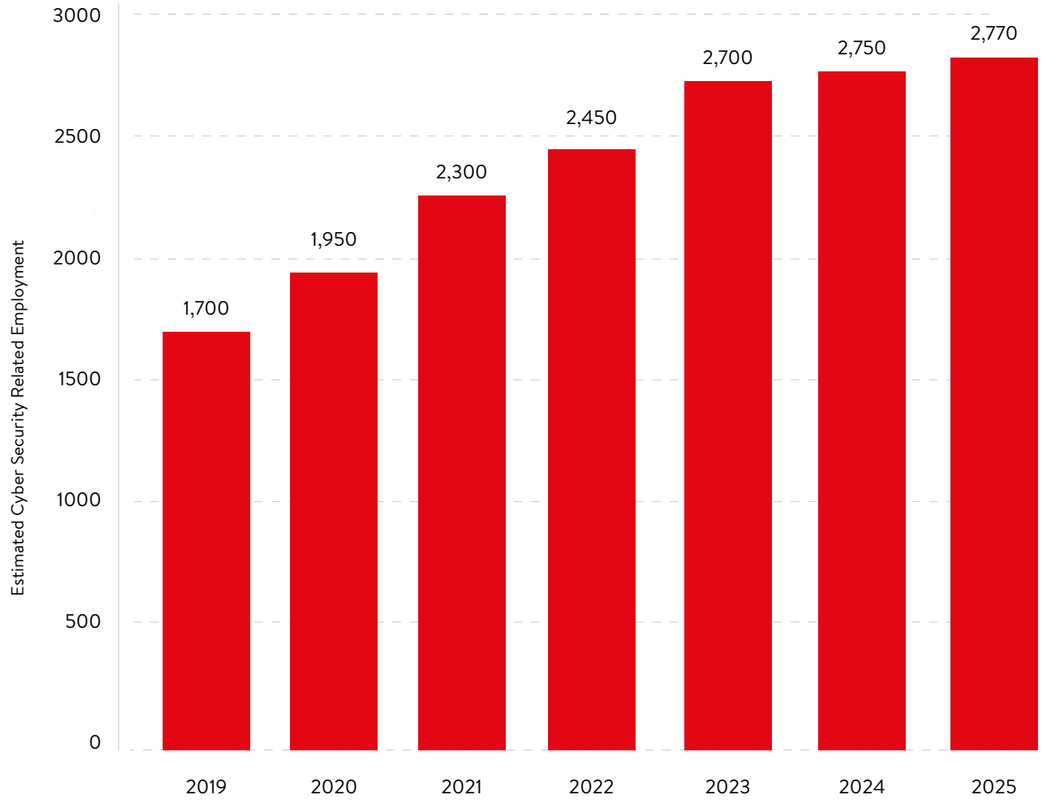
As shown in Section 3.1, demand for new roles (as reflected in job adverts) has also reduced significantly over the past two years. This may have a pincer-effect upon the local cyber security ecosystem, whereby aggregate headcount softens as team sizes tighten, whilst limiting the flow of new opportunities through the skills pipeline, particularly for entry-level staff. Figure 3.1 sets out a time-series for estimated cyber security related employment in Northern Ireland between 2019 and 2025. These estimates have been set out within the DSIT Cyber Security Sectoral Analysis (since 2019) and within NI specific research including previous NI snapshots.

Between 2019 and 2023, headcount increased by 250 people per annum on average, driven by inward investment, and increased recruitment among graduate supply from Queen's University and Ulster University in particular. Initiatives such as Skills Academies supported by the Department for the Economy, alongside inward investors, also supported an increase in the size of the cyber security workforce in this period.

However, between 2023 and 2025, we estimate that growth has broadly flatlined with the overall cyber security workforce consisting of an estimated c. 2,700 to 2,800 people. We set out the potential reasons and implications for this within Section 3.3.

[2] https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

FIGURE 3.1 – ESTIMATED CYBER SECURITY EMPLOYMENT IN NI (2019 – 2025)



Source: Perspective Economics

Figure 3.2 sets out the estimated cyber security headcount based upon where the employer is headquartered globally. For example, if a firm is headquartered in the United States, we apply the headcount for a site in Northern Ireland to be 'US' driven.

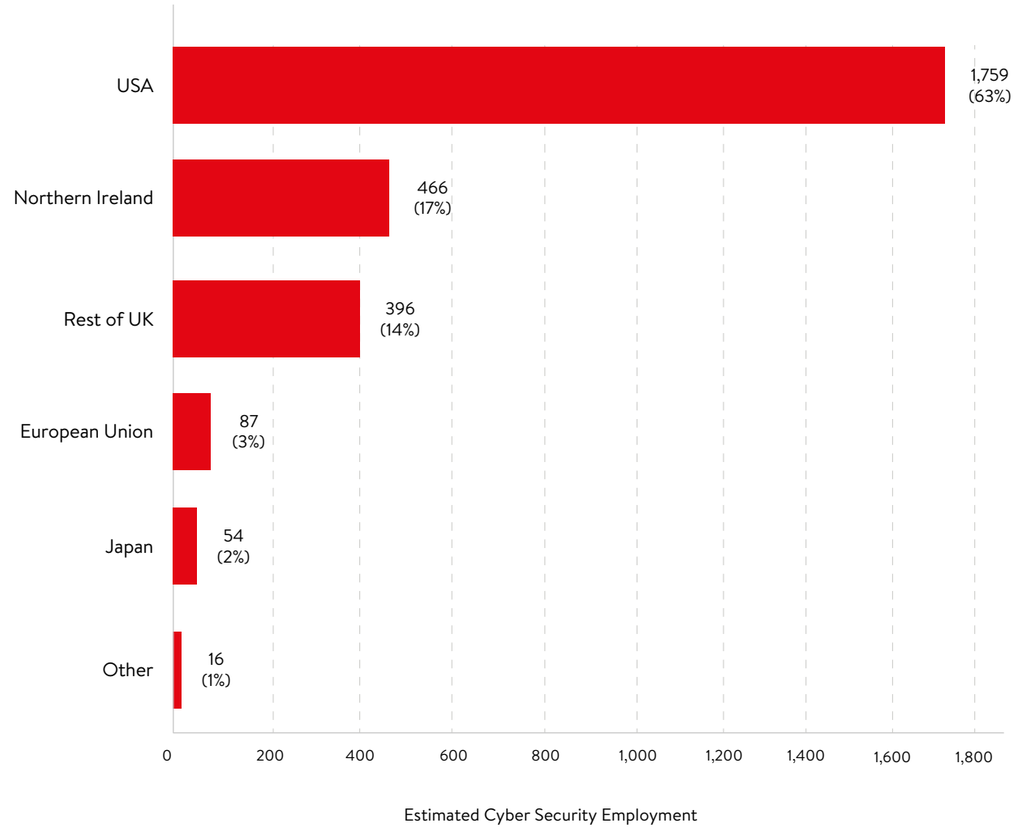
As shown below, we estimate that almost 1,800 roles are supported by US based firms (63%) in NI's cyber security ecosystem. Only one in six (466, 17%) are supported by firms registered and established within Northern Ireland, followed by one in seven (396, 14%) by firms within the rest of the UK. A small number of roles are also supported by EU based firms (including Ireland), Japan, and other countries.

Whilst this concentration of US-headquartered employment reflects Northern Ireland's success in attracting significant foreign direct investment within the cyber security sector, it also presents a structural challenge within the ecosystem. As noted, global investment decisions and efficiency within multinational firms can directly impact local headcount, regardless of the performance or productivity of Northern Ireland-based teams. The sector's exposure to US strategic and macroeconomic conditions may mean that decisions taken in Silicon Valley, Boston, or New York can have direct employment consequences for the Belfast cyber security workforce.

However, it is important to note that this level of US investment also demonstrates Northern Ireland's competitive advantage as a location for cyber security operations. Factors including a strong graduate pipeline from local universities, competitive operating costs, time-zone advantages for US firms servicing both American and European markets, and a stable regulatory environment have all contributed to sustained US interest in the region. Major US cyber security firms have established a range of substantive engineering and research and development capabilities within Northern Ireland.

The modest proportion of roles within indigenous Northern Ireland firms (17%) highlights both a challenge and an opportunity for the ecosystem. Whilst locally headquartered firms may offer some workforce resilience, the domestic cyber security sector remains comparatively small. Strengthening domestic employment opportunities through support for scaling and forming new indigenous firms, encouraging spinouts, and enhanced access to growth capital could help diversify the employment base, whilst also building upon the knowledge transfer and skills development fostered by the presence of leading global firms.

FIGURE 3.2 – ESTIMATED CYBER SECURITY EMPLOYMENT IN NI (2025) BY COMPANY HQ



Source: Perspective Economics

Figure 3.3 sets out the estimated cyber security headcount by firm type and market focus. The analysis distinguishes between 'dedicated' cyber security firms (those whose primary business function is cyber security) and 'diversified' firms (those operating across multiple sectors where cyber security represents one capability among several). Within diversified firms, a further distinction is made between those whose business model includes selling cyber security products or services to the external market, and those maintaining cyber security functions purely for internal purposes e.g. insurance firms with internal cyber risk teams.

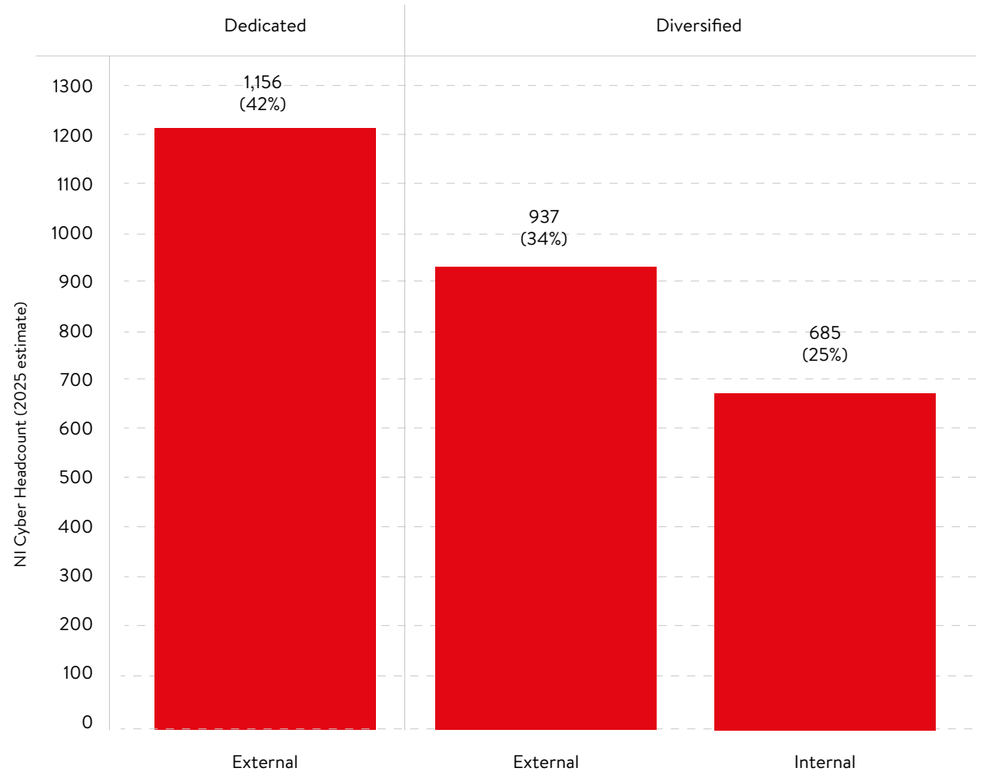
As shown below, we estimate that 1,156 roles (42%) are within dedicated cyber security firms that develop or sell cyber security products or services. A further 937 roles (34%) are within diversified firms whose business activities include offering cyber security products or services externally, meaning that three-quarters of Northern Ireland's cyber security workforce (2,093 roles, 76%) are employed by organisations that directly produce or sell cyber security capabilities. The remaining 685 roles (25%) are within diversified organisations that typically maintain cyber security functions exclusively to protect their own operations, infrastructure, and data.

The predominance of employment within firms that commercialise cyber security reflects Northern Ireland's positioning as a centre for cyber security innovation and service delivery. This has several implications for the ecosystem. Firstly, organisations that sell cyber security products or services externally must remain at the forefront of threat intelligence, new technological advancement, and regulatory compliance in order to maintain competitive advantage. This means that the local ecosystem must have a strong supply of technical and highly talented site leads, be involved in global development, and ensure that the local workforce is exposed to diverse challenge sets across multiple sectors and client environments.

However, it is important to note that organisations focused on supporting external customers may face greater exposure to volatility in demand and economic pressures. As highlighted in Section 3, the global cyber security market has experienced headcount softening in recent years, with firms reassessing their operational footprints and efficiency levels. However, cyber security functions within organisations focused on internal requirements may also demonstrate different employment dynamics, as these capabilities may be exposed to factors such as global outsourcing or automation.

Ensuring an ecosystem with a mix of dedicated and diversified firms can also support workforce development and encourage participation within cluster initiatives such as NI Cyber. Dedicated cyber security firms (42% of headcount) typically offer specialised environments where professionals can develop deep expertise within particular domains such as threat detection, security architecture, or compliance frameworks. Diversified firms, accounting for the majority of roles (58%), may provide exposure to how cyber security integrates with broader business functions, technology stacks, and objectives across different industries. Both firm types contribute complementary strengths to Northern Ireland's cyber security ecosystem.

FIGURE 3.3 – ESTIMATED CYBER SECURITY EMPLOYMENT BY FIRM TYPE & MARKET FOCUS



Source: Perspective Economics

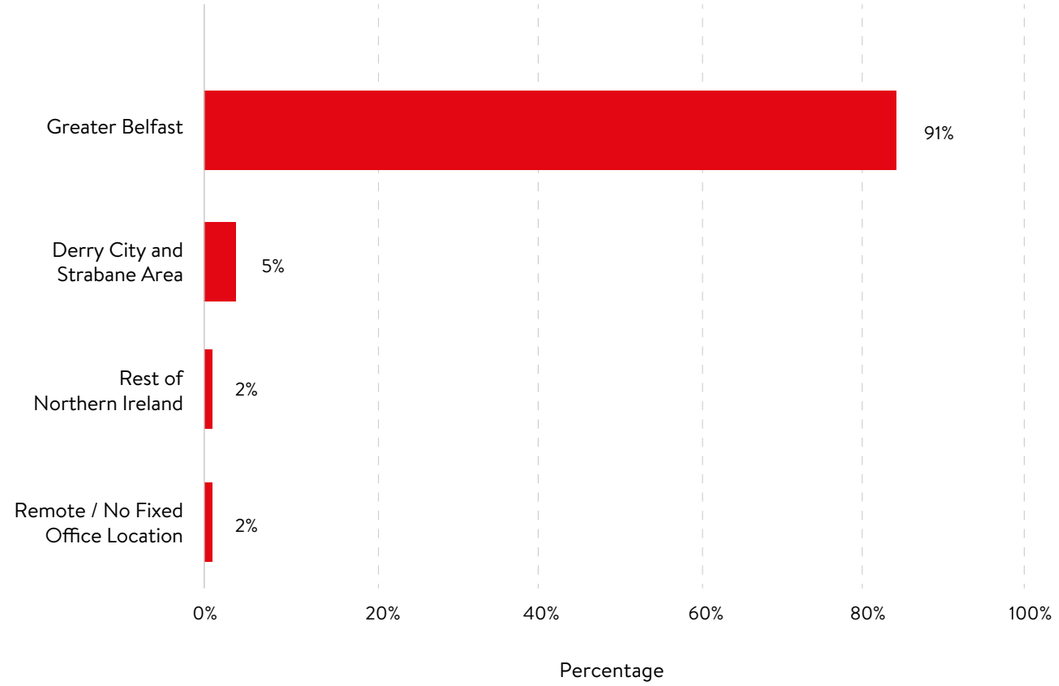
Figure 3.4 sets out the estimated geographic distribution of cyber security employment across Northern Ireland. Locations are based upon each firm's primary operational location for cyber security activities within Northern Ireland.

As shown below, the majority of cyber security roles appear concentrated within Greater Belfast, accounting for 91% of the estimated workforce. The Derry City and Strabane area accounts for a modest 5% of roles, whilst the remainder of Northern Ireland and remote workers without a fixed office location each represent approximately 2% of the cyber security workforce.

This geographic concentration reflects broader patterns within Northern Ireland's knowledge economy, where Belfast's infrastructure, connectivity, graduate talent pool, and agglomeration effects create growth conditions for technology sectors. The presence of both universities, office space, and access to talent all contribute to Belfast's role as the primary location for cyber security operations. For multinational firms establishing operations within Northern Ireland, Belfast offers an appealing destination for accessing talent, infrastructure, and professional services.

However, this concentration presents challenges for regional economic balance and may limit the sector's potential scale. The Derry City and Strabane area, whilst accounting for only 5% of current roles, demonstrates that cyber security capabilities can be established beyond the Greater Belfast area. Further, much of this activity is driven by MetaCompliance, that has successfully scaled operations in recent years.

FIGURE 3.4: ESTIMATED CYBER SECURITY EMPLOYMENT BY NI LOCATION



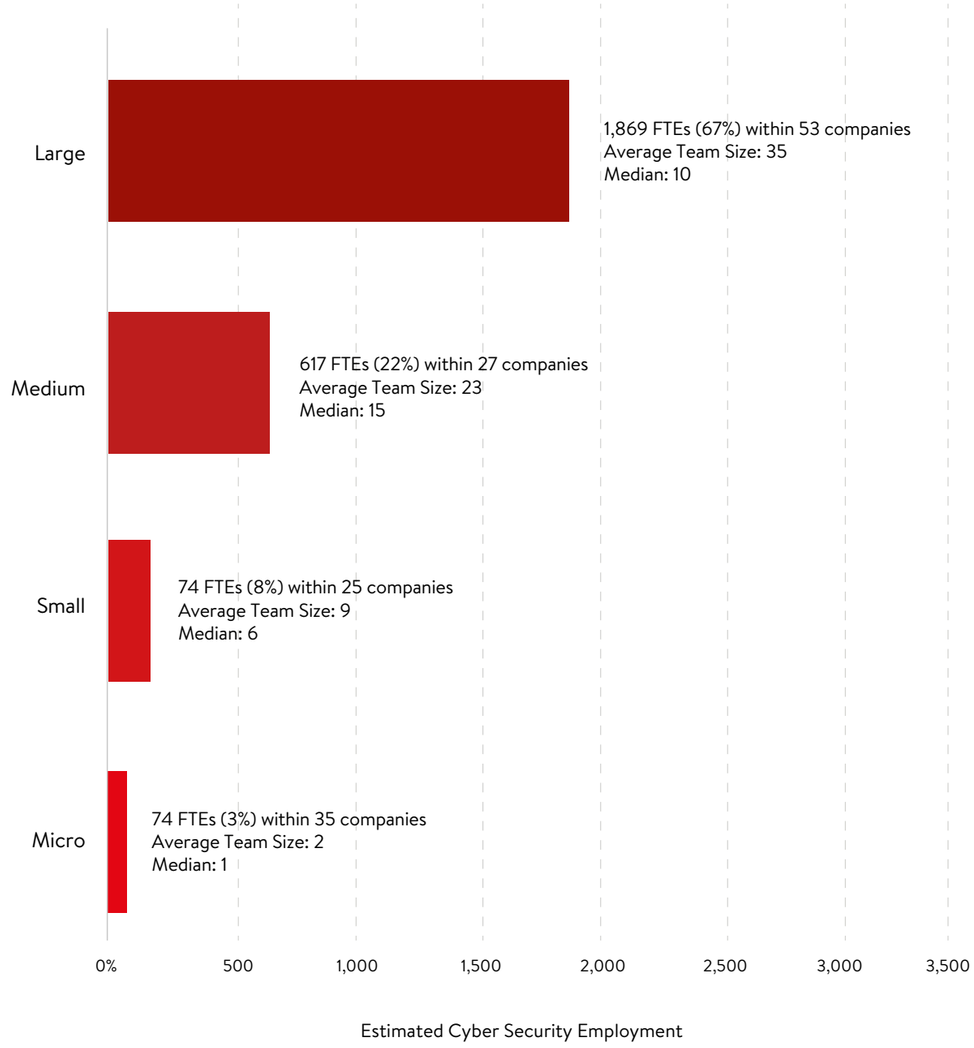
Source: Perspective Economics

Figure 3.5 sets out the distribution of cyber security employment across different firm sizes operating within Northern Ireland. Firms are categorised as Large (50+ cyber security employees), Medium (10-49 employees), Small (5-9 employees), or Micro (fewer than 5 employees), based upon their global presence.

As shown below, large firms dominate the employment landscape, accounting for 1,869 FTEs (67%) across fifty-three companies, driven by several FDI projects. Medium-sized firms employ 617 FTEs (22%) across twenty-seven companies, whilst small firms account for 218 FTEs (8%) across twenty-five companies. Micro firms, despite representing the highest number of companies (35), employ only 74 FTEs (3%) in total.

This chart also highlights average and median team sizes, with a small number of particularly large operations, followed by median cyber security teams of c. 10-15 people within large and medium firms. This also emphasises the challenge for Northern Ireland in that a single large firm changing headcount can offset the growth within multiple smaller firms.
It is notable that there are approximately sixty small and micro firms within the ecosystem, suggesting some appetite for cyber security entrepreneurship and specialist consultancy activities. However, the challenge remains in supporting these firms to grow beyond founder-led operations into scalable employers that can contribute meaningfully to overall headcount and GVA growth.

FIGURE 3.5: ESTIMATED CYBER SECURITY EMPLOYMENT BY FIRM SIZE



Source: Perspective Economics

3.1. DEMAND FOR CYBER SECURITY ROLES

The research team has reviewed online job posting data for the cyber security firms identified within the study over the last five years. This search explores all job postings within key employers identified, and wider use of cyber security job roles (as set out within the DSIT Cyber Skills in the UK Labour Market research definition).

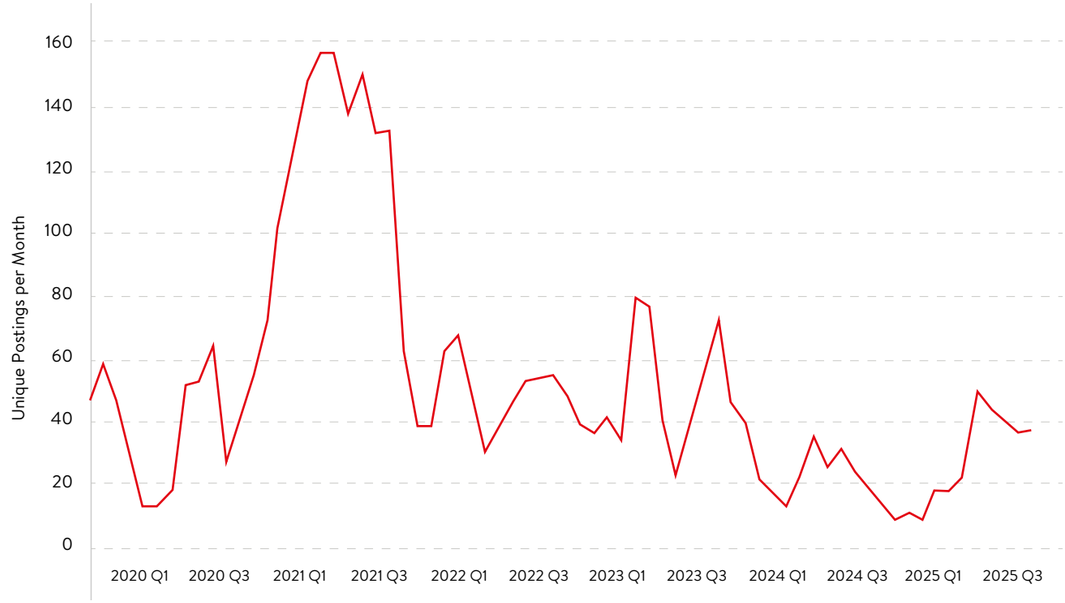
As highlighted in previous studies, the NI cyber security ecosystem demonstrated exceptionally high demand for talent (as reflected in job posting volume) in 2021, with 1,433 unique postings representing a near-threefold increase on 2020 levels. This spike corresponded with a period of rapid expansion among multinational cyber security firms establishing or scaling operations within Northern Ireland. Following this peak, demand moderated, with 2022 and 2023 each recording approximately six hundred postings—representing a 58% reduction from 2021 levels but still above pre-pandemic baseline activity. These trends are set out in Figures 3.6 and 3.7.

In 2024, labour market conditions tightened markedly, with job postings falling to 315 reflecting a 48% reduction compared to the previous year and the lowest level recorded since 2020. Based upon postings recorded to date, we estimate that 2025 will end with approximately 350 postings (c. 30 new roles per month), suggesting that demand has stabilised at this lower level. Some of the companies with highest employment demand in recent years have included Rapid7, Proofpoint, Imperva, Anomali, and Contrast Security.

Whilst we note a substantial reduction in job postings, it is important to contextualise this within broader labour market trends. Similar reductions have been noted across wider software development roles in Northern Ireland, as well as other parts of the wider economy including professional services. This suggests that the cyber security sector's recruitment patterns reflect economy-wide caution regarding headcount growth rather than sector-specific challenges.

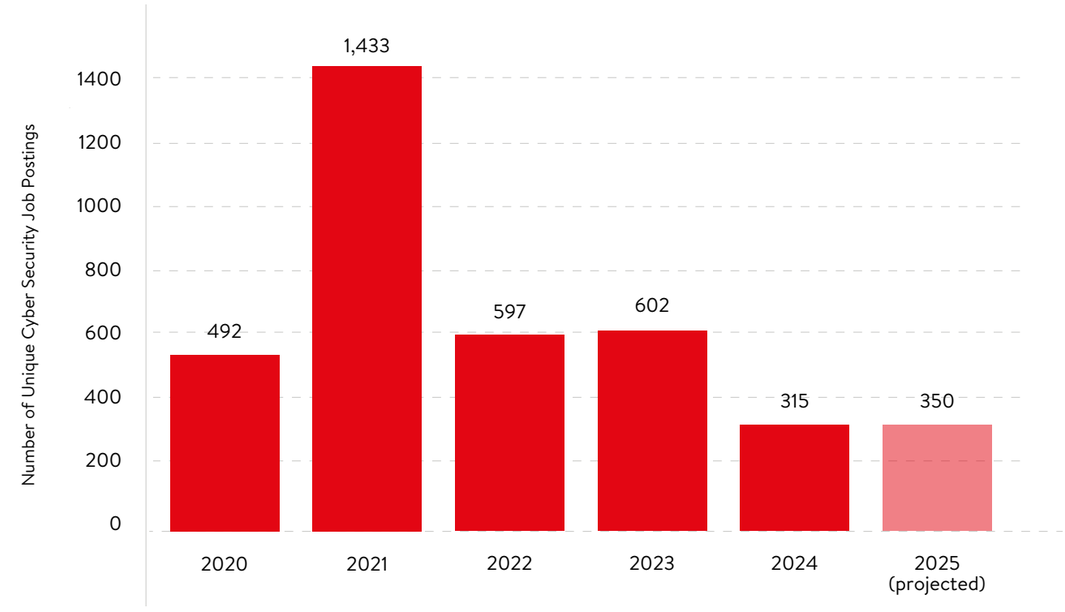
Further, reduced posting volumes should not be interpreted solely as a reduction in recruitment activity. Employer recruitment strategies may have evolved over this period, with firms potentially prioritising different candidate profiles and recruitment channels. There is evidence to suggest that employers are increasingly favouring senior-level hires over graduate or entry-level positions, seeking specialists with proven capabilities rather than building capacity through volume recruitment. Additionally, some firms may be shifting towards more targeted, direct recruitment approaches including executive search or employee referral programmes, which generate lower visibility within public job posting data. For example, firms such as NatWest and Kainos have actively been advertising for cyber security roles in Northern Ireland in 2025 based on our research review.

FIGURE 3.6 – NI CYBER SECURITY JOB POSTING INDEX Q1 2020 – Q3 2025



Source: Perspective Economics, Lightcast

FIGURE 3.7 – NUMBER OF POSTINGS BY YEAR (ESTIMATED)



Source: Perspective Economics

3.2. SUPPLY OF CYBER SECURITY TALENT

Within the previous report, the data highlighted that the majority (over 85% of the NI cyber security workforce) report degree level education[3], and that approximately 25% have Postgraduate Qualifications (Master's, PhDs, and other postgraduate qualifications). Other routes often include those undertaking apprenticeships and or student placements, where a degree award may also be anticipated. Where known, over half of all degrees held by the NI cyber security workforce are in computer science and / or software engineering (52%), approximately 8% are in business and management, 7% are in information technology and systems and 5% are in electronics and electrical engineering. Other degree fields include mathematics and physics, cyber security and digital forensics, data and analytics, artificial intelligence and robotics and other engineering (each between 1% and 3% of those with degree level education).

Based on the previous sample, just under 40% of the workforce have obtained degree level qualifications from Queen's, 29% have obtained degrees from Ulster, and 14% obtained degrees from other UK universities. Just under 5% of the workforce obtained degree level qualifications from international institutions. We also find that an estimated 92% of graduates entering IT roles within the NI labour market from higher education in 2022/23 graduated from Queen's University, Ulster University, or the Open University in Northern Ireland. These proportions emphasise the importance of strong supply from local universities within the NI cyber security ecosystem. The research team has also reviewed Northern Ireland student enrolment and graduation data from the DSIT Cyber Skills in the UK Labour Market 2025 study. The DSIT Cyber Skills research analyses HESA data on Higher Education pathways into cyber security across the UK. The following explores students enrolled in and graduating from cyber security and computer science courses from universities in Northern Ireland. Table 3.1 sets out the number enrolled in and graduating in cyber security[4]and computing related[5] courses in Northern Ireland in 2023/24, highlighting almost 1,700 new graduates across computing, and sixty in cyber security degree pathways.

TABLE 3.1: CYBER SECURITY & COMPUTING STUDENT ENROLMENT AND GRADUATES IN NORTHERN IRELAND UNIVERSITIES (INCLUDES UNDERGRADUATE AND POSTGRADUATE COURSES)

Year	2023 / 24	
	Students Currently Enrolled	Graduates
Cyber Security	200	60
Computing	5,480	1,620
Total	**5,690**	**1,680**

Source: Analysis of data derived from DSIT Cyber Skills in the UK Labour Market 2025

[3] Number of unique workforce records reporting at least 1 degree level qualification via Lightcast.

[4] Cyber security courses defined by the Higher Education Classification of Subjects (HECoS) subject code 100376 as the study of topics around denying access to unauthorised users to computer and information systems, detecting vulnerabilities through ethical hacking and penetration testing and managing the overall information security process.

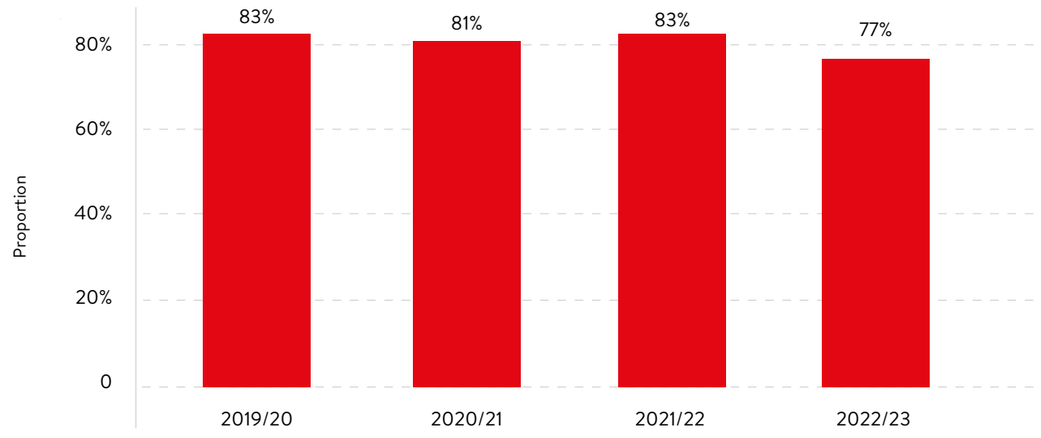
[5] Computing related courses include eight computing courses under the Common Aggregation Hierarchy 11 (CAH11) grouping for computing. This typically includes disciplines such as Computer Science, and Software Engineering.

The most recent HESA Graduate Outcomes (GO) data, which covers graduates from the 2022/23 academic year, surveys graduates about the current outcomes within 15 months of graduating. As shown in Figure 3.8, employment outcomes for Northern Ireland graduates were strong between 2019/20 and 2021/22, with an estimated 83% of graduates securing full-time employment (or undertaking FT employment alongside further study). In this time period, graduates from these courses in Northern Ireland appeared to consistently report higher employment rates in the 15 months after graduating than the UK average, with 84% of graduates in employment or in employment combined with further study, compared to the UK average of 73%. Further, 78% of these graduates in employment report currently being employed in an IT related role (based on 320 responses with a SOC occupation). This highlights a particularly active local labour market across cyber security and the broader IT and software sector between 2021-2023. However, the 2022/23 cohort (i.e. those entering the labour market in 2023/24) shows a softening in employment outcomes. The data suggests the full-time employment rate has reduced from c. 83% to 77%. Further, the absolute number of graduates completing the survey and reporting full-time employment decreased by 31% (from 480 to 330) compared to the previous year, suggesting potential for underemployment or underreported outcomes.

This decline in graduate employment outcomes coincides with the broader labour market challenges identified in previous sections. The 2022/23 cohort would have been seeking employment during 2023 and early 2024—precisely the period when cyber security job postings declined substantially (as shown in Figure 3.7), and overall workforce growth stalled. The combination of reduced opportunities, increased competition for available roles, and a shift away from entry-level recruitment may collectively result in a more challenging environment for new graduates entering the labour market. Whilst Northern Ireland graduates continue to achieve marginally higher employment rates than the UK overall, the steeper decline suggests that local labour market conditions have tightened more severely.

The Graduate Outcomes data also suggests that reported unemployment rates among Northern Ireland cyber security and computer science graduates have increased from 3% to 8% between 2021/22 and 2022/23. Further, analysis of Lightcast job posting data suggests that reported entry-level job postings (roles requiring less than one year's experience) reduced substantially (from 13% of cyber security postings in 2021 to 7% in 2024

FIGURE 3.8: EMPLOYMENT OUTCOMES FOR NI CYBER & COMPUTER SCIENCE GRADUATES



Source: Graduate Outcomes Survey data (Note: Proportion refers to the percentage of relevant NI graduates in FT employment in NI)

3.3. FORECASTING DEMAND TO 2030: UPDATED ASSESSMENT

As noted within the previous section, employment growth within the cyber security sector has significantly softened in recent years and has stalled within the last eighteen months at approximately 2,800 FTEs. In recent years, the NI Strategic Framework for Action in Cyber Security (2017-21), and wider commitments from UK Government, set out an ambitious but considered achievable target of 5,000 FTEs by 2030 in the local industry. This projection was based upon Northern Ireland maintaining or exceeding its prior trend of 200 to 300 new roles per annum—a rate of growth that was sustained between 2019 and 2023.

However, this trend has not materialised beyond 2023, and there are signs of a highly challenging labour market at present. To assess the likelihood of achieving the 5,000 FTE target, and to provide more realistic projections for future workforce scale, this study has developed Monte Carlo forecasting scenarios based upon historical growth patterns, current market conditions, and plausible trajectories for key variables affecting the sector.

Figure 3.9 presents four scenario forecasts to 2030, each with associated confidence intervals and probability assessments regarding achievement of the 5,000 FTE target:

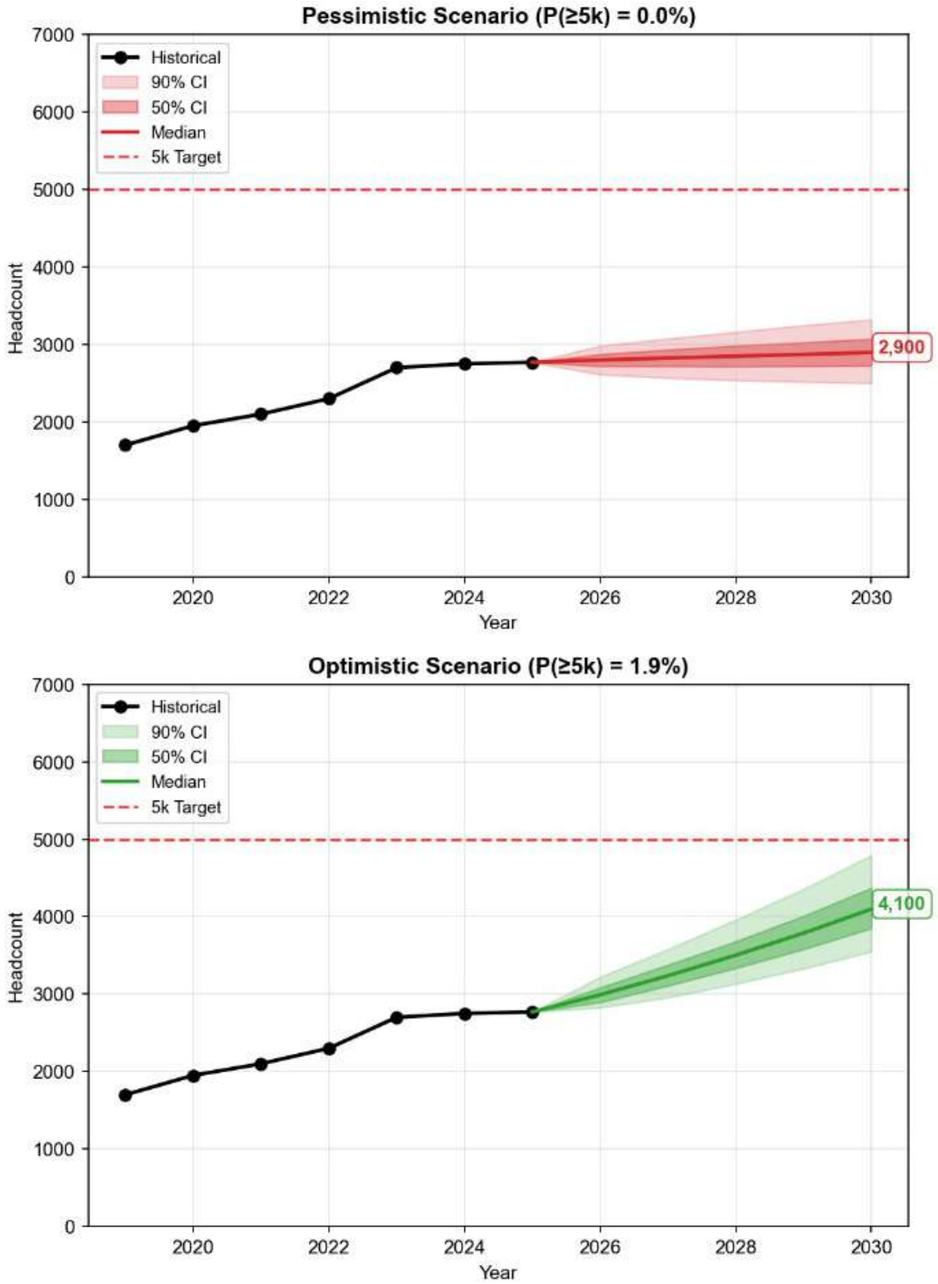
- **Pessimistic Scenario (P(≤5k) = 0.0%):** This scenario assumes continued stagnation or marginal decline in cyber security employment, driven by sustained efficiency measures within multinational firms, limited inward investment, persistent challenges in graduate employment outcomes, and minimal growth within indigenous firms.
- **Base Scenario (P(≤5k) = 0.0%):** The base scenario reflects modest growth rates from current levels, but at lower rates than the 2019-2023 period. It assumes that macroeconomic conditions stabilise, inward investment resumes at moderate levels with new inward investment consisting of dozens of roles per announcement rather than hundreds, and existing major employers maintain current headcount or soften further reductions. Within this scenario, some small-to-medium firms achieve modest scaling, and new micro firms are established. Under this scenario, the median forecast suggests headcount reaching approximately 3,600 FTEs by 2030—representing average annual growth of approximately 100 FTEs per annum, or half the historic rate. Whilst this represents positive trajectory, it remains short of the 5,000 target.
- **Optimistic Scenario (P(≤5k) = 1.9%):** This scenario assumes a return to more favourable conditions, with renewed inward investment from US and international firms, scaling of several indigenous companies, improved entry-level recruitment supporting graduate absorption, public sector activity, and policy interventions that strengthen the ecosystem. Growth rates approach, but do not fully recover to, 2019-2023 levels. The median forecast under this scenario suggests headcount reaching approximately 4,100 FTEs by 2030. Whilst stronger than the base case, even under optimistic conditions the probability of achieving the 5,000 target remains minimal.
- **High Optimistic (Stretch) Scenario (P(≤5k) = 43.5%):** The stretch scenario represents an aggressive growth trajectory requiring multiple positive developments occurring concurrently: significant new inward investment announcements, rapid scaling of indigenous firms supported by enhanced access to growth capital, substantial improvements in graduate pipeline capacity and employment outcomes, and potentially policy interventions such as enhanced R&D incentives or sector-specific support measures. Under this scenario, the median forecast reaches approximately 4,800 FTEs by 2030, with the upper confidence interval extending beyond 5,000. The probability of achieving the target increases to 44%—meaning that under stretch conditions, there is a two-in-five chance of meeting the 5,000 threshold. However, it is important to note that this scenario requires sustained annual growth averaging 300+ FTEs per annum— meeting or exceeding the historical peak growth rates achieved during the most expansionary period of the cyber ecosystem.

We therefore estimate that NI's cyber security ecosystem may reach up to 3,600 FTEs by 2030 under these scenarios, and that economic policymakers may seek to consider underlying factors such as productivity, technical innovation, and the 'stickiness' of investments to date ensuring the ecosystem remains competitive globally. Further, there is a sustained risk that, subject to investment decisions, cyber security employment may be more likely to fall than increase in the next five year period, which increases the impetus to invest and support in research, development, and prime the ecosystem to take advantage of new commercial exploitation in areas such as AI security, software security, connected devices, and more. Several structural factors will determine the sector's employment trajectory, including:

- **Layoffs and efficiency rounds:** The extent to which multinational firms continue to pursue headcount efficiencies will shape employment levels. If efficiency drives continue through 2025-2027, this may suppress growth potential and push outcomes towards pessimistic scenarios. However, increased focus should be placed upon wage and productivity levels, and the medium to long term seniority of these roles.
- **AI and automation:** Emerging automation technologies, including AI driven security tools, may change workforce requirements in different ways across a range of employers. Automation could reduce demand for certain routine security operations roles, often at entry level within areas such as SOC and L1 analysts. However, AI may also increase productivity among experienced leads and enable firms to serve larger markets and clients with existing or reduced headcount. It may also support new specialisms around AI security, AI red-teaming, and adversarial machine learning. This may mean that the nature of roles within the NI ecosystem could shift substantively from number of roles to overall output and outcomes generated by the sector.
- **Market demand:** The overall demand environment for cyber security services will be a critical factor in shaping the ecosystem. Factors including increasing cyber threats, regulatory expansion (such as NIS2 Directive), increasing digitalisation across traditional sectors, and high-profile security incidents which may all create demand pull that supports growth in service roles. This may also be important for the local market, to ensure talented staff are available to support NI SMEs with cyber posture. Conversely, economic constraints limiting client budgets, consolidation within the security vendor market, or technological shifts that reduce per-customer expenditure could all suppress demand. This may be particularly notable within Northern Ireland's focus on areas such as threat intelligence and cloud security.
- **Investment cycles:** Inward investment and venture capital cycles will significantly influence scaling potential, particularly for indigenous firms and new entrants. Improved access to growth capital, successful exits creating reinvestment, or targeted policy interventions supporting scale-ups or incentivising new inward investment may support expansion scenarios.
- **Concentrated risk:** As highlighted in Section 3.1, the concentration of employment within US-headquartered firms creates systemic vulnerability. A small number of large firms adjusting their strategic footprint could eliminate hundreds of roles, regardless of broader ecosystem health. Conversely, announcement of new anchor investments by major firms could support underlying growth. Organisations such as DfE and Invest NI will need to work closely with potential inward investors to demonstrate the overall ability to secure strong labour supply as required.
- **In summary, whilst the 5,000 FTE target remains potentially achievable, the current evidence suggests that more modest growth trajectories are more likely.** Achieving the target would require both a significant improvement in underlying conditions and active policy interventions to address structural constraints within the ecosystem. **Absent such developments, a realistic planning assumption for 2030 would be a cyber security workforce in the range of 3,500 to 4,000 FTEs.**

FIGURE 3.9: EMPLOYMENT FORECASTS FOR NI CYBER (TO 2030)

NI Cyber Headcount Monte Carlo Forecasts to 2030



4. CUSTOMERS, PARTNERSHIPS AND DEMAND

This section explores key customers, use cases, partnerships and demand for the cyber security products and services developed in the NI ecosystem. As noted previously, the NI cyber security ecosystem contains a wide range of vendors with highly varied business models and approaches. For example, this can include:

- Dedicated (or pure-play) cyber security firms focused on product and research and development activity;
- Dedicated cyber security managed services and advisory services that support a range of organisations with their cyber security posture and provision;
- Diversified firms with technical cyber security capabilities and external clients, such as large consultancy firms with cyber audit and risk services; and
- Diversified firms with cyber security capabilities used internally e.g. manufacturing, financial and professional services, or food production firms with cyber security teams designed for internal use.

Collectively, this highlights the diversity of provision within the local ecosystem, as well as several routes to market. This breadth of activity represents a structural opportunity for the NI cyber security ecosystem, recognising that cyber security is a broad domain encompassing novel product development, managed security services, consultancy and advisory functions, and in-house defensive capabilities across multiple sectors. This diversity can also provide economic resilience, as if demand softens in one segment, others may remain stable or even expand to absorb talent and expertise.

As noted previously, Northern Ireland's cyber security ecosystem is highly shaped by the role of multinational firms, and this means that the region is directly and indirectly supporting and servicing a wide range of global export markets. However, stimulating local demand is also important. The region's base, comprising thousands of SMEs across manufacturing, agrifood, professional services, retail, and other sectors face increasing cyber risk exposure. Many of these organisations may lack the scale or expertise to maintain dedicated security functions, creating an opportunity for accessible, affordable managed services and advisory support, as well as strengthening local supply chains in critical sectors.

Beyond commercial growth, there is a wider imperative to embed cyber security awareness and capability across Northern Ireland's public and private sectors. Government departments, local councils, health trusts, schools and universities, the voluntary sector, and critical infrastructure operators all require robust cyber defences and appropriately skilled and aware workforces. There is an ongoing need to ensure a stronger cyber security culture through awareness programmes, skills initiatives, and accessible expertise, which helps protect essential services and builds collective resilience. A diverse ecosystem, with multiple service offerings, is best positioned to support this mission.

We explore the dynamics of the local market, including key business partnerships and customers, accreditations and awards secured by the NI cyber security ecosystem.

4.1. CUSTOMERS & TECHNOLOGY PARTNERS

The research team has reviewed web data (where available) for dedicated cyber security firms active within the Northern Ireland ecosystem. This includes where dedicated firms mention partnerships, customers, or case studies from other businesses or organisations. This provides some insight into how firms engage with the market; however, we note that for multinational firms, customers may include non-NI teams working with non-NI customers.

	No. of Partnerships Identified
Local (NI Headquartered)	174 (14 providers)
FDI / Global	1,066 (22 providers)

For local NI headquartered firms, we find several examples of partnerships across local organisations (e.g. securing systems for local schools and public sector clients), external sales and partnerships with firms across Great Britain and Ireland, and wider export and partnership activity with larger global vendors.

We set out some examples below:

FIGURE 4.1 – NI CYBER SECURITY CASE STUDIES

leaf Enhancing cyber resilience for Ulster Rugby

Ulster Rugby relies on Kingspan Stadium as its operational centre. With tens of thousands of fans, international broadcasters, and multiple systems running simultaneously, the club recog-nised a need to modernise its infrastructure to minimise outages and safeguard against cyber attacks. Belfast-based Leaf IT, Ulster Rugby's long-standing IT and infrastructure partner[6], designed and implemented a new network architecture supported by enhanced firewall securi-ty and built-in fail-safes, ensuring systems remain operational even in the event of issues.

Leaf IT continues to deliver ongoing cyber security services including email filtering and disas-ter recovery, as well as Microsoft Cloud services that underpin the club's email, intranet, and wider cloud infrastructure.

"We are grateful for Leaf IT's continued support, which ensures Kingspan Stadium remains a world-class venue capable of hosting top-tier rugby fixtures. It's fantastic to work with a local company on this project, and I encourage other businesses across Ulster to reach out and contribute to the ongoing success of the club." Bryn Cunningham, Head of Operations and Recruitment, Ulster Rugby

[6] https://leaf-it.com/case-study/ulster-rugby-2/

MetaCompliance Enhancing cyber resilience for Ulster Rugby

Low employee engagement in cyber security awareness training presented a risk to the DAERA's ability to achieve ISO27001 certification. The Department partnered with MetaCompliance to implement a more engaging training approach, including 'nano videos' that emphasised the significance of cyber security both at work and at home. The training adopted an 'anytime, anywhere' learning model, allowing employees to access content at their convenience. MetaCompliance also streamlined the Department's incident reporting processes. These interventions increased employee engagement rates to 90%, strengthening DAERA's cyber security operational capability and supporting its ISO27001 certification efforts.

Cyberspark CyberSpark Group receives DSIT and NCSC endorsement as CyberFirst member

CyberSpark, a Belfast-based cyber security academy, received endorsement from the Department for Science, Innovation and Technology (DSIT) and the National Cyber Security Centre (NCSC), becoming a member of the CyberFirst programme.

CyberFirst is a government-backed outreach and education programme designed to create opportunities for young people in cyber security careers, supporting students from all backgrounds to consider careers in cyber security and related fields. CyberSpark provides foundational and advanced cyber training, preparing school and university students for careers in IT and cyber security through hands-on courses and industry-recognised certifications.

The organisation has also launched the UK and Ireland's first 'Cyber Battle'[7] competition, an initiative aimed at positioning Northern Ireland as a global leader in cyber security education and workforce development. Open to those aged 14-24, teams are challenged to defend against simulated cyber-attacks across a series of bootcamps.

"It's great to be recognised as helping in the huge task of making the United Kingdom a cyber-safe nation. We look forward to a long and rewarding relationship." [Richard Coates, CEO, CyberSpark Group]

[7] https://cyberspark.group/belfast-company-launches-uk-and-irelands-first-cyber-battle-competition/

Outsource Group becomes exclusive Palo Alto Networks partner for the island of Ireland

Antrim-based Outsource Group partnered with US firm Palo Alto Networks[8], one of the world's leading cyber security firms to become the only Palo Alto Cortex Managed Security Service Provider Partner (MSSP) on the island of Ireland in 2024. The arrangement is expected to generate several million pounds in new business, and enables Outsource Group to sell, con-figure and deploy Palo Alto Networks' suite of AI-powered cyber security products across both Northern Ireland and Ireland with full vendor support.

Outsource Group invested over £1 million in its journey to achieve this status, including in-vestment in staff, training, and innovative technology, achieving a range of technical certifica-tions and completing a rigorous Palo Alto Networks assessment process.

Shailesh Rao, President for Cortex at Palo Alto Networks, visited Outsource Group in Belfast to mark the beginning of the partnership. "The rigorous assessment undertaken by Palo Alto of Outsource Group's expertise and capabilities and the ultimate agreement to enter into a working partnership and formal appointment of Outsource as the only Cortex MSSP on the island is a strong endorsement of our strategic security first approach." [Terry Moore, CEO, Outsource Group]

Building cyber security capability across Ireland

Nemstar[9], a Belfast based specialist in cyber security training, has delivered cyber security qualifications and capability building programmes to organisations across Northern Ireland and the Republic of Ireland. Founded by Sean Hanna, four-time recipient of the EC Council's global cyber security trainer of the year award, Nemstar has trained over 13,000 professionals globally. Recent clients include the Garda Síochána Ombudsman Commission (GSOC)—the independent body responsible for handling complaints about members of Ireland's national police service—and Atlantic Technological University (ATU), one of Ireland's largest technological universities.

"We recently availed of Cyber Security training from Nemstar, the trainer was excellent, extremely professional and very knowledgeable, creating a positive learning experience, with very practical/ real-life examples where required." [David McCormack, Head of Information and Communications Technology, Garda Síochána Ombudsman Commission]

[8] https://osgroup.co.uk/news/outsource-group-partners-with-palo-alto/
[9] https://www.nemstar.com/

Securing Northern Ireland's first autonomous transport system at Belfast Harbour[10]

Belfast Harbour is developing the 'Harlander' project—one of the UK's first fully driverless passenger transport systems on public roads—to provide last mile connectivity across the Harbour Estate from Titanic Quarter railway station to Thompson Dock. With visitor numbers predicted to rise from 3.6 million to over 5.6 million by 2035, establishing secure autonomous transport is a critical component of the Estate's sustainable transportation plan.

ANGOKA was selected to provide cyber security for the project following a competitive process issued by the Centre for Connected and Autonomous Vehicles (CCAV), joining a consortium that includes BT, HORIBA MIRA, and REE Automotive. ANGOKA is responsible for the cyber security of remote vehicle operations and system-wide Vehicle Security Operations Centre (Vehicle-SOC) capabilities, preventing unauthorised access and ensuring passenger safety. The first Belfast Harbour shuttle services entered pilot passenger service in 2025.

"ANGOKA is delighted to be a part of the Harlander consortium and look forward to contributing with our unique cyber security technology to protect critical data and to ensure the safe and secure operation of autonomous vehicles. We are excited to help build a state-of-the-art live showcase on our doorstep which will put Belfast right at the forefront of smart city innovation." [Yuri Andersson, Executive Director, ANGOKA]

Moving beyond local dedicated firms, analysis of partnerships and integrations across global firms with cyber security operations in Northern Ireland emphasises a highly interconnected ecosystem, with local teams embedded within global technology supply chains and partner networks. We note that this includes a mix of customers, partnerships, and technology stacks mentioned by providers; and therefore, should be viewed as indicative. However, we find:

Platform concentration: Firms such as Microsoft appears as a partner or integration point across the majority of firms analysed (64%), reflecting its importance in enterprise IT and the strategic importance of Azure and Microsoft 365 integrations for cyber security vendors. Similarly, AWS features prominently across multiple firms including Agio, Contrast Security, Imperva, Proofpoint, SmartTech247, Theta Lake, and Veeam highlighting the importance of cloud security capabilities. Splunk, Palo Alto Networks, and ServiceNow also appear repeatedly, suggesting that Northern Ireland-based teams are routinely working with and integrating into the infrastructure that underpins global enterprise security.

Global integration: Many of the firms listed maintain extensive integration partnerships with other cyber security vendors, creating a layered ecosystem where NI-developed capabilities feed into broader security stacks. For example, Anomali maintains integrations with a wide range technology partners spanning threat intelligence providers[11] (e.g. Recorded Future, Mandiant, CrowdStrike), SIEM platforms (Splunk, IBM QRadar, Microsoft Sentinel, Elasticsearch), and network security vendors (Palo Alto Networks, Fortinet, Zscaler). Whilst these partnerships are

[10] https://www.angoka.io/projects-1/zero-carbon-world
[11] https://www.anomali.com/marketplace/threat-intelligence-feeds

global in nature, the presence of engineering, product development, and customer-facing teams in Northern Ireland means that local staff are actively contributing to integration development, partner enablement, and joint go-to-market activities. Further, several firms maintain partnerships with global system integrators and consultancies, including Accenture, Deloitte, Capgemini, Cognizant, and PwC. These relationships are significant as they provide routes to market for NI-developed products and services into large enterprise and public sector contracts globally. Further, firms such as Cloudsmith are also leading in software security, working with engineering teams in leading firms such as Carta and Humanising Autonomy.

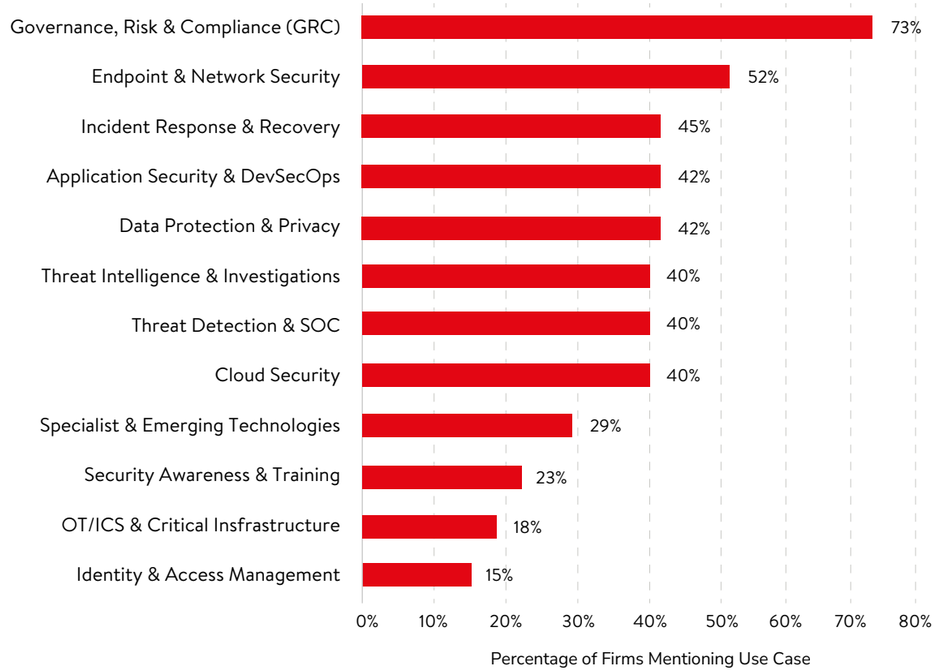
Emerging technology partnerships: Several firms demonstrate partnerships in emerging technology domains. Ampliphae (now Arqit) maintains relationships with the European Space Agency, Northrop Grumman, and multiple government agencies around quantum-safe encryption. ANGOKA works with Innovate UK, CCAV, and defence organisations on connected and autonomous vehicle security. These partnerships can help to position Northern Ireland within leading-edge security domains likely to grow over the coming decade.

4.2. USE CASES

Review of company web data can also provide insight into how companies actually use and deploy cyber security capabilities to support their end customers. This can demonstrate how cyber security is used across the local ecosystem and help to identity areas of strength and opportunity based on existing capabilities.

Figure 4.2 sets out the proportion of firms within Northern Ireland's cyber security ecosystem that reference capabilities within a range of twelve classified use case categories. This analysis is based upon publicly available information including company websites, case studies, and product and marketing content. A firm is counted once per category regardless of the number of discrete use cases referenced. It is important to note methodological limitations in this analysis. Larger firms may often maintain more web data relating to their capabilities, potentially inflating their coverage across multiple categories. Conversely, smaller firms may describe their offerings in terms that do not fully capture technical depth or specialist focus. Further, the absence of a capability from public materials, or the inability to draw on web data, does not necessarily mean that the firm does not deliver this use case or solution.

FIGURE 4.2 – PERCENTAGE OF FIRMS REPORTING EACH USE CASE CATEGORY



Source: Perspective Economics (n = 62 market suppliers (all NI and dedicated global) with 284 unique identified use cases for products and services in cyber security)

As shown below, Governance, Risk and Compliance (GRC) is the most referenced use case capability by 73% of firms. This includes supporting firms with regulatory compliance (e.g. GDPR, NIS2, PCI DSS), certification support (ISO 27001, Cyber Essentials), audit and assurance services, risk management frameworks, and policy development. This is a broad area but reflects NI's strength as a destination for ensuring risk and compliance functions are in place and offers a route for further growth as more global firms seek to develop compliance and risk teams in Northern Ireland.

This is followed by Endpoint and Network Security (52%), including areas such as endpoint detection and response, firewall management, email security, and remote working infrastructure. This category reflects the continued importance of foundational security, particularly for managed service providers servicing local SME clients where endpoint and network protection are primary requirements in demand.

Specialist and Emerging Technologies (29%) includes cyber security capabilities in areas such as autonomous vehicles, quantum, AI/ML security, software security, defence and space, and health technology. This reflects a cohort of firms with specialised capabilities in novel areas of cyber security. CSIT's Cyber-AI Hub works closely with several of these firms including Rapid7 (using agentic AI for threat detection), Pytilia (context aware vulnerability detection and mitigation), and ControlSoft (threat detection for industrial control systems), and is exploring opportunities with Arqit (quantum safe encryption) .

Security Awareness and Training (23%) also reflects the presence of dedicated awareness and training

providers (e.g. Instil (acquired Vertical Structure), Nemstar, MetaCompliance) alongside managed service providers and IT consultancies offering awareness and training as part of broader offerings (e.g. Instil, Kainos).

4.3. MARKET DEMAND & OPPORTUNITIES

Northern Ireland has established a distinctive position within the UK cyber security landscape, characterised by substantial inward investment from US-headquartered firms and world-class research infrastructure at CSIT. However, there remain opportunities to increase the number of new startups, increase investment in new security research and innovation, and improve levels of local adoption of cyber security standards to help ensure the long-term sustainability of the ecosystem.

We set out four areas for increasing opportunities for growth: stimulating local demand through policy mechanisms; capturing national security and defence opportunities aligned with Northern Ireland's industrial base; encouraging startups and strengthening the pipeline from research to commercialisation; and positioning the region to lead in emerging specialist domains.

Stimulating Local Demand

As of April 2023[12], Northern Ireland accounted for approximately 1% of UK Cyber Essentials certified organisations, with c. 270 certified organisations (including public, private, and voluntary organisations). This is disproportionately low compared to its share of the UK business population (c. 2.9% of all VAT / PAYE registered firms). In comparison, Wales has almost 1,000 certified organisations (4% of all certified organisations, with c. 4% of the business population.

This represents a potential cyber security resilience gap within Northern Ireland, with low levels of voluntary take up of the Cyber Essentials scheme. There are several policy levers that could help stimulate take up and demand including mandating standards (similar to PPN 09/23 in the UK) within Northern Ireland public procurement for government suppliers to hold Cyber Essentials or equivalent to secure contracts, and the sustained provision of funding and support to smaller firms and voluntary organisations to access support e.g. extension of schemes such as the NI Cyber Essentials Funded Programme[13].

Further, ensuring that local firms can identify and access market providers that can support longer-term cyber security posture (e.g. via managed services, support with software security, pen testing etc.) may also help to build longer-term revenue and growth in the domestic market.

National Security and Defence

Northern Ireland maintains significant defence and aerospace industrial presence through firms such as Thales, Spirit AeroSystems, and Harland & Wolff. ADS (NI) estimates that the aerospace, defence, security, and space sectors in Northern Ireland contribute over £1.9bn to the NI economy each year.

The UK's National Security Strategy (2025) sets out UK Government plans to increase investment as a percentage of GDP in defence to c. 5% by 2035. Through this increased investment, there will be direct and supply chain opportunities for Northern Ireland to help embed digital security within national security and defence projects. It is estimated the Ministry of Defence already spends c. £140m with suppliers in Northern Ireland[14], and there could be opportunities for further growth in areas such as OT security, embedded systems, and secure communications.

Ensuring Northern Ireland is an attractive location for investment in national security and defence can help support long-term supply chains and create further opportunities for the local cyber security research and labour ecosystem. Thales also announced they plan to invest over £100m in NI operations, supporting over two hundred jobs in Belfast[15].

[12] https://www.gov.uk/government/publications/cyber-essentials-scheme-impact-evaluation/cyber-essentials-impact-evaluation

[13] https://www.nibusinessinfo.co.uk/content/ni-cyber-essentials-funded-programme

Encouraging Startups and Commercialisation

Analysis of the Northern Ireland cyber security ecosystem suggests a small rate of new startups being formed in cyber security, with single-digit numbers of new local cyber security firms established annually in recent years. The majority of these are service-oriented businesses (consultancy and managed services) rather than product or IP-based ventures.¬ This may constrain the ecosystem's capacity for innovation and limits pathways for research commercialisation.

Addressing this gap will require deliberate intervention to support venture creation at the earliest stages. In recent years, initiatives including CSIT Labs have demonstrated that structured support for spinning out research-based companies can generate product-focused startups, with firms including Affyon, Ditaca, Sirona, Liopa, Sensurity and Cognition Video, which focused on delivering cyber security solutions involving content inspection, visual speech recognition, cryptography technologies, intrusion detection and platforms for automatic and intelligent image and video processing all being formed. Further, one of CSIT's most successful spinouts, Titan IC, was acquired by Mellanox and subsequently NVIDIA – resulting in NVIDIA's R&D presence expanding in Belfast.

Increasing the capability to build and support new ventures in cyber security could create a pipeline of innovative ventures capable of progressing to national growth programmes such as Cyber Runway and securing new growth in NI. Ensuring that there are wider supports, including direct financial support, to encourage new startups should be a priority for local economic growth.

Beyond creating new firms, there exists opportunity to attract experienced entrepreneurs and technical leaders to establish operations in Northern Ireland. Alumni from successful indigenous firms or FDI operations may represent a talent pool with sector expertise, commercial networks, and often capital to invest. Systematic outreach by organisations such as Invest NI and NI Connections may help to encourage this cohort to establish their next base in Northern Ireland, supported by appropriate incentives and connections to local research and talent, which in turn could accelerate the formation of experienced founder-led businesses.

Specialist Domain Opportunities

Northern Ireland should position deliberately within emerging domains where research capabilities, industrial context, or existing firm presence create foundations for distinctive advantage.

AI Security and Assurance. The establishment of the Cyber-AI Hub positions Northern Ireland at the forefront of UK AI security research. As organisations implement AI systems under increasing regulatory scrutiny, demand for AI security assessment, red-teaming, and assurance services will grow substantially. Expansion of the Hub into other sectors, such as security domains in fintech and advanced manufacturing on , could help further commercial AI security capabilities alongside research infrastructure, and in turn, establish Northern Ireland as a centre for AI regulatory, risk, audit, and testing services. AICC is working with SMEs across multiple sectors, some of which could benefit from deep-tech collaboration with cyber security experts at CSIT through the Cyber-AI Hub; similarly, CSIT can direct companies to AICC for support on introducing AI to their business. The Cyber-AI Hub Director is on the board of AICC and has regular engagement, which is helping to ensure alignment across the two initiatives.

Semiconductor Security. The Northern Ireland semiconductor cluster, identified within the National Semiconductor Strategy and anchored by firms including Seagate and IceMOS, has particular strengths in photonics and sensor technologies through the Smart Nano NI initiative. Hardware assurance – verifying chip integrity in critical infrastructure and defence applications – represents a growing requirement in a range of industries and

[14] https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html

[15] https://www.bbc.co.uk/news/articles/cgl0z7gxpg2o

applications, including IoT, Cyber Physical Systems, Advanced Manufacturing and CNI. Building on its expertise in hardware security, CSIT prioritised Semiconductor Security as a key focus within its 2022–2027 research and innovation programme. Demonstrating national leadership in this domain, CSIT has led the UK Research Institute in Secure Hardware and Embedded Systems (RISE) since 2017. Funded by EPSRC and NCSC, RISE has established a vibrant UK hardware security community, and has developed strong national and international partnerships, including with the US and Germany. It has also strengthened UK skills in semiconductor security through dedicated training programmes and seasonal schools, while actively shaping policy in collaboration with DSIT. Future opportunities include establishing a Semiconductor Security Hub (akin to the Cyber-AI Hub), accelerating research commercialisation and co-creating solutions with industry partners, strengthening NI's competitive edge in this sector.

Operational Technology and Industrial Security. As industrial digitalisation accelerates and NIS2 implementation imposes enhanced security obligations on operators of essential services, demand for OT security expertise spanning manufacturing, energy, transport, and critical infrastructure will grow. NI Cyber and CSIT has already explored a number of these challenges within all-island advanced manufacturing cyber security research. Building on this established capability to develop specialisation in secure industrial control systems could position Northern Ireland within this significant area of opportunity.

5. INVESTMENT LANDSCAPE

This section explores investment in the NI cyber security ecosystem via two main indicators, namely external investment from Venture Capital investors (as recorded by Beauhurst), and levels of inward investment from FDI (as recorded by FDI Markets). We note that each of these indicators may only apply to a small sample of firms in the region given the overall size of the NI cyber security ecosystem, and as such, caution should be exercised with respect to trend-based analysis, as figures can be skewed by individual deals or announcements. However, this does provide some insight into overarching investment activity, scale, and sentiment within the local sector.

Since 2020, dedicated cyber security firms registered in Northern Ireland have raised over £80m across twenty-two deals. We summarise the number of deals and amount raised below. As noted within the DSIT Cyber Security Sectoral Analysis reports, overall VC investment into cyber security firms has decreased year on year since 2021, and this trend is similar within Northern Ireland, with only a single VC deal (officially announced) in both 2024 and 2025.

5.1. VC INVESTMENT

Since 2020, dedicated cyber security firms registered in Northern Ireland have raised over £80m across twenty-two deals. We summarise the number of deals and amount raised below. As noted within the DSIT Cyber Security Sectoral Analysis reports, overall VC investment into cyber security firms has decreased year on year since 2021, and this trend is similar within Northern Ireland, with only a single VC deal (officially announced) in both 2024 and 2025.

Year	Number of Deals	Amount Raised
2025 (to date)	1	£18.1m
2024	1	£2m
2023	4	£28m
2022	3	£4.8m
2021	7	£24.7m
2020	6	£2.5m

Source: PE analysis of Beauhurst Data

This data may indicate a potential challenge for the NI ecosystem both with respect to deal flow, and the overall number of firms positioned for investment readiness. This suggests that increasing the number of early-stage product-driven startups within the NI ecosystem should be a clear priority for stakeholders.

In March 2025, Cloudsmith (a Belfast-based cloud-native artifact management platform focusing on software supply chain security) raised a $23m (£18.1m) Series B funding round. During this announcement, Cloudsmith reported that they ‘grew nearly 150% last year’ and that ‘new capital from this oversubscribed funding round will go towards expanding sales, marketing, and customer success teams, innovation in software supply chain security product features, and investing in AI R&D’.

This is a key example of how indigenous firms can be supported to grow over several years, secure external investment for growth, and scale globally whilst expanding their NI headcount and overall value-add for the local economy.

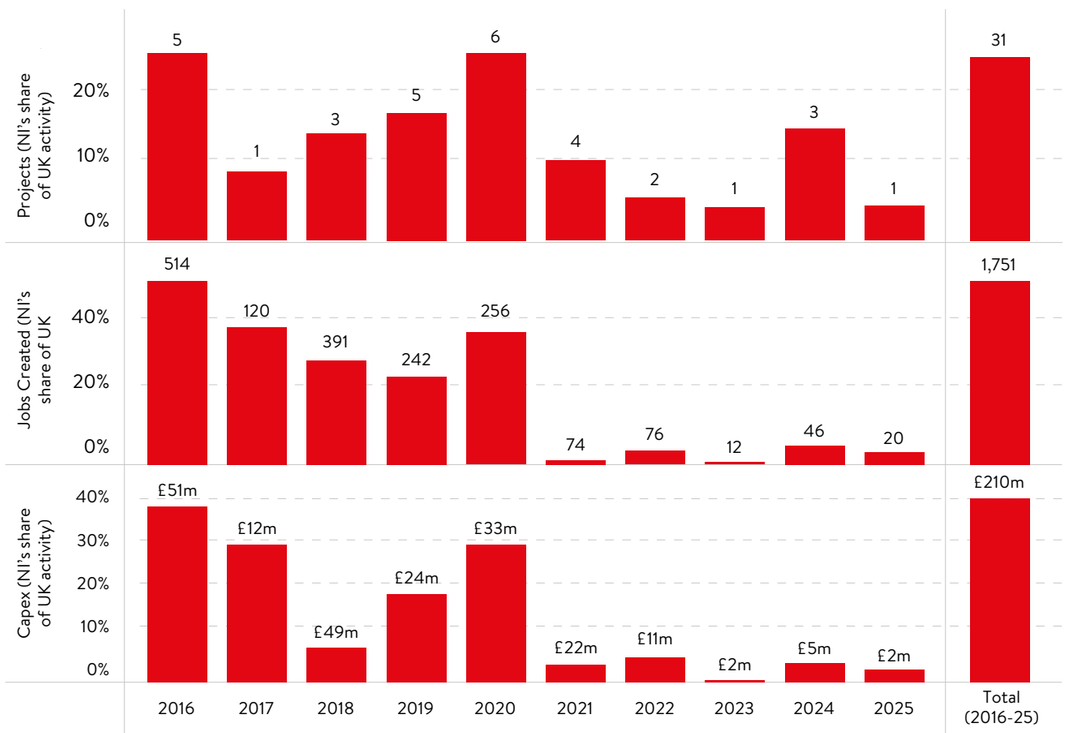
5.2. FOREIGN DIRECT INVESTMENT

In the last decade, Northern Ireland has been noted as a leading European investment location for US cyber security firms and for software development overall.[16] This activity has translated directly into increasing the size and scale of the cyber security workforce and embedding specialisms in areas such as threat intelligence and cloud security.

We explore this data over the last decade to explore how inward investment has changed over time.

This analysis uses FDI Markets and a search for cyber security related inward investment projects. This typically focuses on dedicated cyber security firms and may not capture elements of inward investment from broader sectors such as fintech that may also recruit cyber security talent. However, this does provide insight into the longitudinal trends regarding inward investment projects. As shown below, inward investment activity was particularly significant in Northern Ireland between 2016 – 2020, with firms such as Rapid7, Black Duck (since acquired by Synopsys), Imperva, Signifyd, ProofPoint, Aflac, Contrast Security, and Microsoft all announcing significant investments in Belfast. It is also impressive to note that despite only consisting of c. 3% of the UK's business population, Northern Ireland typically received up to 25% of all UK inward announcements in cyber in this period.

FIGURE 5.1 NUMBER OF FDI PROJECTS, NUMBER OF JOBS CREATED, & CAPEX INVESTMENT



Source: Perspective Economics, FDI Markets (please note that 2025 covers January to October only)

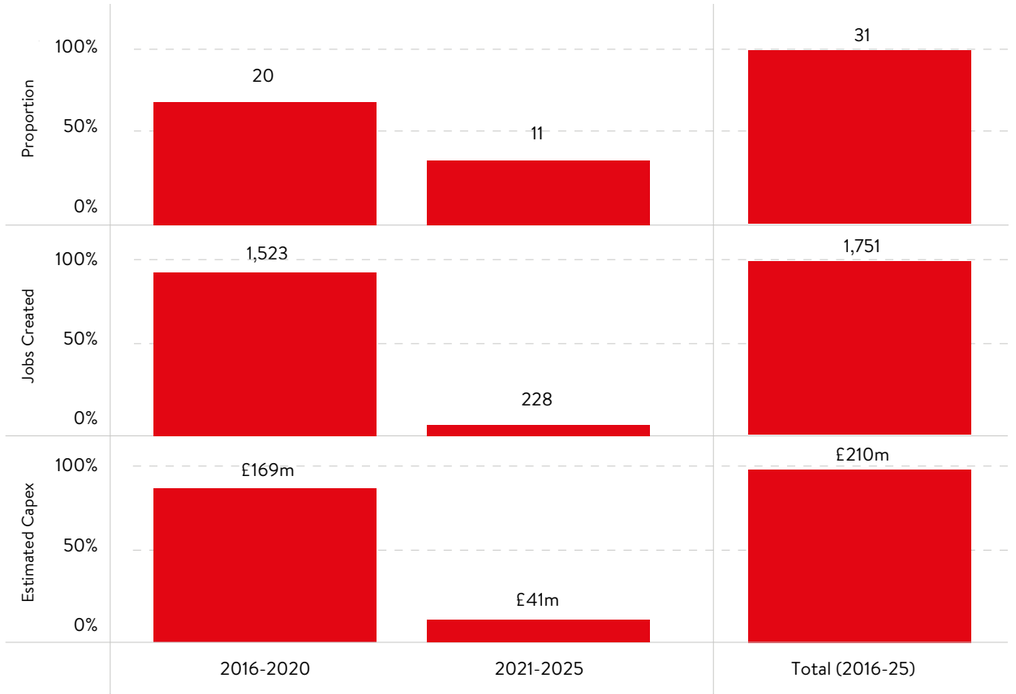
[16] https://www.investni.com/international-business/our-sectors/technology

However, announced FDI has fallen significantly since 2021 in Northern Ireland cyber security projects. In the two five-year periods (2016-2020 vs 2021-2025 YTD), we note:

- A 45% reduction in announced new investment projects (from 20 to 11)
- An 85% reduction in newly announced roles (from 1,523 to 228)
- A 76% reduction in estimated Capex (estimated capital expenditure from investment projects)

This comes amidst a backdrop of greater volatility within global FDI driven by macroeconomic conditions, as well as tensions in global trade.[17]

FIGURE 5.2 FDI PROJECTS, JOBS AND CAPEX (2016-2020, 2021-2025)



Source: Perspective Economics, FDI Markets

[17] https://www.oecd.org/en/topics/foreign-direct-investment-fdi.html

6. RESEARCH & EDUCATION

CSIT is the UK's Innovation and Knowledge Centre for cyber security. Its mission is to couple major research breakthroughs in the field of secure information technologies with a unique model of innovation and commercialisation to drive economic and societal impact. CSIT brings together expertise in academic research and applies this through its extensive business engagement and engineering activity.

6.1. RECOGNITION OF RESEARCH QUALITY

CSIT has also been recognised by the National Cyber Security Centre (NCSC) for the high quality of its research and education activity, holding both Academic Centre of Excellence in Cyber Security Research (ACE-CSR) and Academic Centre of Excellence in Cyber Security Education for which it received Gold Award recognition in 2024. Further, the Queen's University Belfast MSc in Applied Cyber Security has also been recognised as an NCSC-certified degree programme.

CSIT plays a key role in the development of the cyber security ecosystem, through:

- Supporting a **sustainable talent pipeline**
- **Championing diversity** in cyber security talent
- Strengthening **academic-industry partnerships**
- Promoting NI as a **cyber security destination for R&D**

6.2. SUBSTANTIVE KNOWLEDGE CONTRIBUTIONS

Since the previous snapshot, researchers at Queen's have published almost dozens of academic outputs with a particular focus on:

- Applying AI to support secure control systems and embedded environments.
- Effectively integrating cyber-physical systems.
- Securing next-generation wireless technologies.

Figure 6.1 overleaf provides several examples of the important contributions that the Northern Ireland cyber security research ecosystem is making to the wider national and international cyber security knowledge landscape.

FIGURE 6.1 – RESEARCH CASE STUDIES

DANGER-IoT: Advancing state-of-the-art IoT malware protection

As malicious malware attacks on IoT devices continue to rise, the need for effective detection solutions is critical. While considerable research has focused on traditional devices like PCs and smartphones, those approaches don't translate well to IoT devices, such as medical equipment, smart home components, autonomous vehicles, and industrial systems, which are diverse and have limited computing power. Together with Rochester Institute of Technology (RIT), Northeastern University (NE) and University College Cork (UCC), in November 2024, Queen's researchers secured £270k via the US-Ireland R&D Partnership Programme[18] to develop a new IoT malware detection method that is universal, efficient, and robust. The project kicked off in April 2025 and will run for three years.

TruDetect: Trustworthy deep learning-based hardware Trojan detection (2023-26)

The semiconductor supply chain encompasses overseas foundries, third-party IP, and untrusted test facilities, and exposes silicon chips to hardware-based security threats including counterfeiting, IP piracy, and hardware trojans (malicious circuit modifications). As part of RISE (the UK Research Institute in Secure Hardware and Embedded Systems), CSIT researchers secured EPSRC funding for the TruDetect project, which aims to develop a trustworthy deep learning-based hardware Trojan detection system. The project, led by Professor Máire O'Neill, Dr Ihsen Alouani, and Dr Niall McLaughlin, aims to create detection systems that can be integrated into Electronic Design Automation (EDA) tools, incorporating novel countermeasures against adversarial attacks and explainable AI techniques to provide comprehensive analysis of system behaviour.

CyberUnite: Cyber security of cross-border critical infrastructure (2026-2029)[19]

CyberUnite is a €4 million research project aimed at fortifying the cybersecurity of cross border critical infrastructure across the island of Ireland, funded by the Irish Government's Shared Island Initiative. The project is co led by Professor Donna O'Shea of the University of Limerick and Dr. Kieran McLaughlin of Queen's University Belfast's Centre for Secure Information Technologies (CSIT), with consortium partners Munster Technological University (MTU), University College Cork (UCC) and industry partner Gas Networks Ireland (GNI). CyberUnite's mission is to develop resilient and adaptive cyber defences for shared social and economic systems, particularly critical sectors, including energy and utilities.

[18] The US-Ireland R&D Partnership is a tri-jurisdictional alliance which supports collaborative research with the potential to generate valuable discoveries and innovations which are transferable to the marketplace.

[19] https://www.ul.ie/news/ul-researchers-to-lead-eu4-million-cross-border-cybersecurity-project

6.3. RESEARCH & INNOVATION INITIATIVES

Launched in 2023, CSIT's £10m Cyber-AI Hub continues to make strong progress in deepening collaborative partnerships with R&D-intensive cyber companies. The Hub is training a cohort of 15 PhD students and forty master's students in cyber security and AI, with an expanding portfolio of industry collaborators contributing to research directions and providing placement opportunities. In late 2024, CSIT supported the launch of the Laboratory for AI Security Research (LASR), developed in partnership with GCHQ and the Alan Turing Institute, positioning Northern Ireland at the forefront of AI safety research within the UK.

In 2024, CSIT secured a share of £8M in funding from the UK government to establish a new Centre for Doctoral Training (CDT) in Future Open Secure Networks (CDT-FORT) in partnership with the University of Surrey. This CDT will create a community of at least fifty postgraduate researchers across the two locations, who will become industry-conscious thinkers and leaders with unique expertise that encompasses cyber security, wireless communications, networking, and AI. This provides fully funded PhD opportunities in four research themes, including Space Communications and Security, Trustworthy AI for Secure Future Open Networks, Secure and Trustworthy Hardware, and AI-Assisted Physical Layer Security. Beyond cyber security-specific programmes, Queen's researchers contribute to broader quantum technology research through participation in the QEPNT (Quantum Enhanced Positioning, Navigation and Timing) Hub, based at the University of Glasgow, as one of five quantum hubs launched with £106 million EPSRC investment. Queen's researchers also collaborate with industry partners engaged with the EPSRC Centre for Doctoral Training in Applied Quantum Technologies creating potential pathways for quantum-safe communications and quantum applications relevant to defence and critical infrastructure sectors.

6.4. SUSTAINED FOCUS ON EDUCATION & SKILLS

Cyber security remains a key priority for growing the region's economy, and as such continues to garner unwavering support through education and skills initiatives at all levels. Education providers continue to work together to ensure a high-quality and sustainable pipeline of cyber security talent and skills that can support growth and development ambitions across the private, public, and academic sectors.

As of mid-2025, a total of 31 NI schools and colleges maintain CyberFirst accreditation from the National Cyber Security Centre. The CyberFirst EmPower Girls initiative has grown since its inaugural event in 2024, when 250 school-aged girls from twelve schools attended the first event at Windsor Park. In April 2025, the second EmPower Girls event saw six hundred Year 8 girls from twenty-two schools across Northern Ireland gather at ICC Belfast, supported by over fifty industry companies, academic institutions, and government bodies. Post-event surveys from the inaugural 2024 event demonstrated that 80% of participants were more likely to consider pursuing a career in technology and cyber security following their attendance, indicating meaningful impact on perceptions and aspirations.

As one of Cisco's largest 'Networking Academy Support Centres,' the Open University in Belfast is working with all six of Northern Ireland's Further Education (FE) colleges to equip students with industry-aligned skills in networking, cyber security, and programming.

7. FINDINGS & RECOMMENDATIONS

This report has provided an updated assessment of Northern Ireland's cyber security ecosystem, highlighting both the substantial progress made over the past decade and the structural challenges that may shape its trajectory to 2030. This section synthesises the key findings and sets out recommendations to support sustained growth, diversification, and high-value activity within the sector.

7.1. KEY FINDINGS

Employment Growth Has Stalled, But Productivity Remains Strong

Northern Ireland's cyber security workforce has reached approximately 2,778 FTEs as of November 2025, representing marginal growth since 2023. This contrasts sharply with the period between 2019 and 2023, when the sector added an average of 250 roles annually. Job posting volumes have declined by 48% since 2023, and graduate employment outcomes have softened, with full-time employment rates falling from 83% to 77% between 2021/22 and 2022/23 cohorts.

However, it is important to recognise that these trends reflect global labour market conditions rather than specific weaknesses to Northern Ireland. The ISC2 global workforce study reports null growth in the worldwide cyber security workforce in 2024, with reductions in both European and North American markets. Layoffs and efficiency measures have been reported by 25% of cyber security firms globally, and hiring decisions are being restrained.

Whilst headcount growth has softened, we note that the underlying productivity of the Northern Ireland ecosystem remains strong. With advertised salaries in excess of £53,300, and overall direct Gross Value Added in excess of £258m, the cyber security ecosystem offers Northern Ireland thousands of high-value engineering, research and development, and security operations centre roles with global significance.

Inward Investment has reduced

Foreign Direct Investment in Northern Ireland cyber security projects appears to have reduced significantly since 2021. Comparing two five-year periods (2016-2020 vs 2021-2025), FDI project announcements have fallen by 45%, and newly announced roles have declined by 85%.

This reduction coincides with broader global trends in FDI volatility, but it provides a challenge to how the NI ecosystem positions itself for long-term strategic growth. Between 2016 and 2020, several global cyber security firms established substantial operations in Belfast, creating anchor investments that have supported graduate absorption and skills development. We understand that Northern Ireland remains an attractive destination for ongoing FDI, but projects may have lower levels of headcount announcements. As such, strength in certain technical and commercial domains, and diversification to ensure all sectors benefit from cyber security skills will be crucial to sustain and renew headcount growth.

Achieving 5,000 FTEs by 2030 Will Be Challenging

Previous strategic frameworks set out an ambition of 5,000 cyber security roles in Northern Ireland by 2030. Based upon current labour market conditions, macroeconomic and technological trends, and forecasting scenarios set out in this study, this target appears increasingly challenging to achieve.
Under a base scenario—assuming moderate inward investment, stable headcount among existing large employers, and modest growth within indigenous firms—the median forecast suggests the workforce reaching approximately 3,600 FTEs by 2030.
However, it is important to note that headcount is not the only measure of ecosystem success. Increased productivity driven by AI and automation, higher average salaries reflecting seniority and specialisation, and deeper integration within emerging domains such as AI security, quantum, and operational technology may all contribute to increased economic value in future. This reflects an opportunity for stakeholders

within the NI cyber ecosystem to consider the long-term targets, strategy, and 'model' for the sector in the years ahead.

Indigenous Firm Growth Remains Limited

We estimate that 17% of Northern Ireland's cyber security workforce (c. 466 FTEs) are employed by locally headquartered firms. Whilst there are several examples of successful local companies—including MetaCompliance, Cloudsmith, Instil, and others—the rate of new company formation remains modest, with single-digit numbers of new cyber security startups established annually in recent years.

We also note that venture capital investment in Northern Ireland cyber security firms has also declined, with only one officially announced deal in each of 2024 and 2025 to date. This suggests potential medium-term challenges with respect to deal flow and the overall number of firms positioned for investment readiness.

Strengthening the indigenous firm base through enhanced support for startup development should be a clear priority for the ecosystem.

Research Excellence Provides a Strong Foundation for Igniting Growth

Northern Ireland continues to maintain world-class cyber security research capabilities through CSIT, recognised by the NCSC as an Academic Centre of Excellence in both research and education. The establishment of the Cyber-AI Hub, participation in the LASR initiative, and the role of CSIT in several UK leading research initiatives all position the region at the forefront of emerging security domains. However, translating research excellence into commercial growth requires sustained investment in spin-out support, access to seed and early-stage funding, and mechanisms to scale successful ventures within the region.

Encouraging local demand for cyber security

Northern Ireland accounts for approximately 1% of UK Cyber Essentials certifications despite representing c. 3% of the UK business population. This suggests that local adoption of cyber security standards remains lower than in comparable regions, representing both a resilience gap and a small but untapped market opportunity for managed service providers and advisory firms. Stimulating local demand through policy mechanisms—including mandating standards within public procurement, providing funded support for SMEs and voluntary organisations, and raising awareness of regulatory obligations could create sustained revenue opportunities for indigenous firms whilst strengthening the overall cyber resilience of the Northern Ireland economy.

7.2. RECOMMENDATIONS

The findings set out above suggest that Northern Ireland's cyber security ecosystem requires deliberate intervention to support diversification, stimulate local demand, and position the region within emerging high-value domains. We set out five priority recommendations below.

Recommendation 1: Stimulate Local Demand

Northern Ireland should prioritise increasing cyber security adoption among local businesses, public sector organisations, and voluntary sector bodies. This will strengthen overall resilience, create sustained revenue opportunities for managed service providers and advisory firms, and reduce dependency on global export markets for growth.

Actions:

- Mandate Cyber Essentials or equivalent certification for all public sector suppliers, following the approach taken in PPN 09/23 for UK Government procurement.
- Extend funded support programmes (such as the NI Cyber Essentials Funded Programme) to enable SMEs and voluntary organisations to access certification and advisory services.
- Develop sector-specific guidance and support for industries facing new regulatory obligations, including energy, transport, health, and digital infrastructure providers.
- Support the development of an accessible directory of local cyber security service providers to enable SMEs to identify and engage with appropriate support.

Recommendation 2: Invest and Prioritise Emerging Technical Domains

Northern Ireland should focus on establishing distinctive capabilities within emerging cyber security domains where research infrastructure, industrial context, and existing firm presence create foundations for competitive advantage.

Priority domains could include:

- AI Security and Assurance: Building upon CSIT, the Cyber-AI Hub and LASR to establish Northern Ireland as a centre for AI security assessment, red-teaming, regulatory compliance, and assurance services.
- Semiconductor and Hardware Security: Connecting CSIT's hardware security research and work on UK RISE with industry to develop verification capabilities relevant to defence, critical national infrastructure, and high-assurance sectors.
- Operational Technology and Industrial Security: Leveraging existing CSIT's cyber security research and NI's advanced manufacturing industrial base to develop specialisation in secure industrial control systems, smart infrastructure, and connected devices.
- Quantum: Leveraging CSIT's expertise in post quantum encryption, research collaborations within quantum technology hubs, and supporting firms such as Arqit, to position Northern Ireland within quantum-secure communications and security of quantum systems.

Actions:

Develop targeted inward investment propositions for firms operating within these specialist domains or seeking to develop new capabilities.

- Support firms to access research partnerships aligned to these areas.
- Continue to invest in PhD and postgraduate training programmes with specialisations relevant to these domains.

Recommendation 3: Strengthen Support for New Startups

The ecosystem would benefit from direct intervention to increase the rate of new venture creation, support early-stage firms to achieve investment readiness, and enable scaling.

Actions:

- Provide or broker early-stage funding specifically for new cyber security product ventures, recognising that product and research-led startups often require longer development timelines than typical software-as-a-service businesses.

- Provide direct support or initiatives to encourage new start-ups (similar to Founder Labs)

- Establish spin-out support mechanisms (building upon initiatives such as CSIT Labs) to translate research progress into commercial ventures.

- Ensure that growth-stage firms have access to appropriate funding, commercial support, and talent to scale domestically.

Recommendation 4: Identify National Security and Defence Opportunities

The UK Government has committed to increasing defence spending to 5% of GDP by 2030. Northern Ireland's existing defence and aerospace industrial base creates opportunities to embed cyber security capabilities within national security supply chains, to support national procurement of defence capabilities, and to translate this expertise to other critical national industries, such as food processing and health & life sciences.

Actions:

- Identify cyber security capability requirements within defence projects and national security programmes.

- Explore opportunities for Northern Ireland to develop, host or support sovereign cyber security capabilities relevant to UK national security and dual-use applications.

Recommendation 5: Sustained Investment in Research, Innovation, and Skills

Research excellence has been foundational to Northern Ireland's cyber security ecosystem. Sustained investment in CSIT, industry partnerships, and skills development remains essential to long-term sustainability and attractiveness of the region.

Actions:

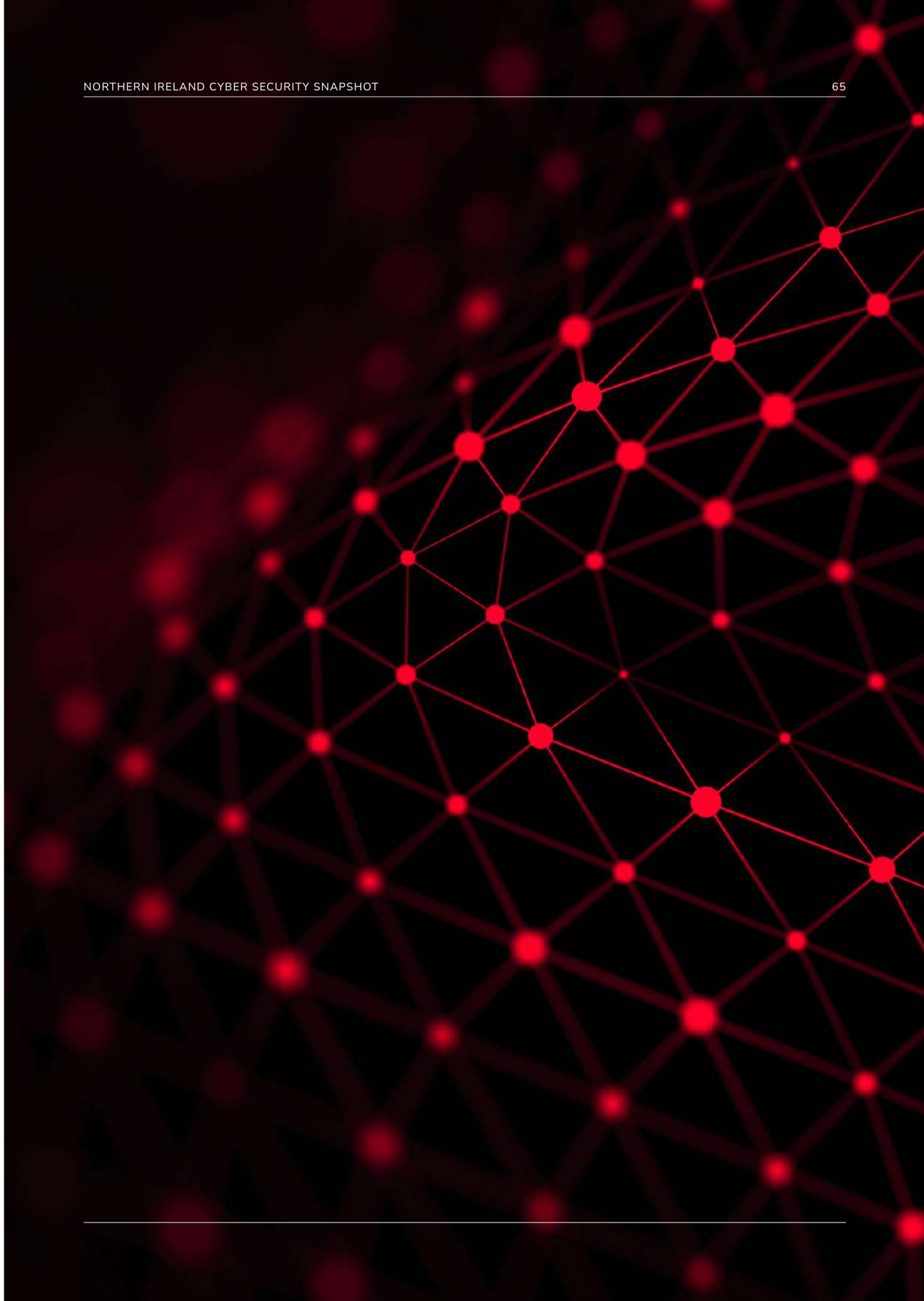
- Ensure sustained funding for CSIT beyond the current IKC phase to maintain research capabilities, industry partnerships, and postgraduate training.

- Expand collaborative research programmes that connect academic expertise with industry challenges, ensuring that research outputs are designed with bleeding-edge technical development or commercial applications in mind.

- Maintain involvement with national initiatives such as CyberFirst and NCSC Cyber Advisor programmes, and direct support for studentships to ensure a sustainable talent pipeline.

- Support mid-career upskilling pathways to enable professionals from adjacent disciplines (e.g. software engineering, data analytics, IT operations) to transition into cyber security roles or achieve security related accreditation.

Northern Ireland's cyber security ecosystem has achieved remarkable growth over the past two decades, establishing the region as a recognised international centre for cyber security research, innovation, and commercial activity. Whilst current macroeconomic conditions present challenges, there remains substantial opportunity to deepen capabilities, increase productivity, and position the region within emerging high-value domains. Achieving this will require continued collaboration across government, academia, and industry to stimulate local demand, support indigenous firm growth, and ensure that Northern Ireland remains an attractive destination for cyber security investment and talent.



QUEEN'S UNIVERSITY BELFAST | CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

perspective economics

Centre for Secure Information Technologies (CSIT)
Queen's University Titanic Quarter
Belfast
BT3 9DT

Telephone: 028 9097 1700
Website: http://go.qub.ac.uk/csit
LinkedIn: www.linkedin.com/company/csit-qub/