Northern Ireland Cyber Security Sector Snapshot 2021

May 2021

Authors:

David Crozier (CSIT)

Sam Donaldson & Conor Tinnelly (Perspective Economics)

Contents

1 Executive Summary

Research Overview

Following the publication of the DCMS UK Cyber Security Sectoral Analysis (2021), the Centre for Secure Information Technologies (CSIT) and Perspective Economics have undertaken this deep-dive research to provide:

- An economic analysis of Northern Ireland's cyber security market, setting out known cyber security companies within Northern Ireland, and a profile of cyber security employment and economic activity within the region.
- An independent analysis of the NI cyber security sector that considers potential market value (measured in Gross Value Added), and considers local economic impact and growth rates.
- Recommendations to help refine future proposals and provide evidence based assessments of the economic and societal impact of supporting the cyber security ecosystem in Northern Ireland.

Number of Companies and Employees working in Cyber Security:

Overall, this review of the Northern Ireland cyber security ecosystem identifies 104 firms offering cyber security products and services. **We estimate that these firms currently employ 2,299 Full Time Equivalent (FTE) cyber security professionals (as of April 2021).**

The average salary for an NI cyber security professional (2020) is estimated at £48,400 (DCMS, 2021). This means that the sector **currently generates in excess of £110m in annual salaries** within the NI economy.

We also estimate that the Gross Value Added (GVA) per cyber security employee in Northern Ireland is approximately £70,000 (DCMS, 2021). This means that the direct **Gross Value Added (GVA) contribution of the cyber security industry in Northern Ireland is estimated at £161m per annum**.

The methodology used to identify cyber security businesses and employees operating within Northern Ireland is consistent with the UK Cyber Security Sectoral Analysis 2021 research undertaken for DCMS. However, we classify the cyber security products and services offered by firms operating in Northern Ireland into six distinct areas, as the research team has identified relative strengths in the following areas:

- Managed Security Service Provision and Advisory Services
- Risk, Compliance and Fraud
- Securing Applications, Networks and Cloud Environments
- Operational Technology, Security and Connected Devices
- Threat Intelligence, Monitoring, Detection and Analysis
- Identification, Authentication and Access Controls

As set out in the report, the Northern Ireland cyber security ecosystem has a unique mix of strengths in these six areas, reflected by the number of companies and employees specialising in each area.

The Northern Ireland ecosystem offers sufficient scale and depth of expertise in each of these categories, which offers considerable potential for commercial application.

An international destination for cyber security investment

The growth of the Northern Ireland cyber security ecosystem has arguably been advanced by international interest in the role of Belfast and Derry/Londonderry as cities with emerging technology specialism, backed by the role of CSIT as a key asset with respect to talent pipeline, and collaboration in R&D and engineering projects.

Further, the intensity of Foreign Direct Investment into the Northern Ireland cyber security ecosystem is strong. The United States is a key investment partner, with 37 firms employing 1,432 cyber security professionals (62% of NI based cyber security employment).

	United States:	Northern Ireland:	Rest of UK:	Rest of World:
Number of Companies	37 *(36%)*	39 *(38%)*	18 *(17%)*	10 *(10%)*
Cyber Security Employment	1,432 *(62%)*	482 *(21%)*	228 *(10%)*	157 *(7%)*

This reflects the pivotal role of FDI in shaping the sector to date. Further, analysis of Invest NI open data highlights that Invest NI has provided c. £27m worth of funding to support the creation of over 1,300 cyber security roles in NI sector between 2015 and 2020, with increased focus on promoting job creation with this investment, and increased engagement with US firms.

Significant economic opportunity for Northern Ireland:

The importance of growth in the sector is recognised in the NI Executive's New Decade, New Approach document, and within the Department for the Economy's 10X Economy - an economic vision for a decade of innovation and its Economic Recovery Action Plan.

The New Decade, New Approach deal sets out commitments to promote Northern Ireland as a global cyber security hub, recognising and building on NI's *"blend of world-class talent, leading forensic science expertise and tech research excellence"*, to achieve 5,000 cyber security job roles by 2030.

This is further emphasised in the Economic Recovery Action Plan setting out free online access to skilled training within a cyber security job vacancy platform.

Economic modelling and potential for growth:

Economic modelling was undertaken to estimate the value of cyber security employment to the Northern Ireland economy at current levels and for 2030 projections.

Currently the sector generates **in excess of £110m in annual salaries** and **Gross Value Added (GVA) per employee is approximately £70,000** (DCMS, 2021). This means that the direct **GVA contribution of the cyber security industry in Northern Ireland is estimated at £161m per annum**.

This is important for three key reasons:

- Firstly, Northern Ireland has experienced long-standing challenges with respect to private sector productivity and salary levels. Cyber security offers a considerable economic opportunity for the region, with salaries well in excess of NI private sector median levels[1], and offer a strong platform for growing productivity in the NI private sector. However, these salary levels remain competitive within a UK and international context, and are conducive to attracting new investment, and expanding indigenous firms.
- Secondly, Northern Ireland has set an ambitious jobs target (5,000 FTEs by 2030). The expansion of available roles, alongside ensuring a sustainable talent pipeline, will help to substantially boost the lifetime earnings of thousands of individuals brought into the sector.
- Finally, this economic activity is largely driven through external investment into the region. Northern Ireland teams are developing solutions used world-wide, and ultimately increasing external sales and exports for Northern Ireland and the broader UK economy.

The research team has explored three potential scenarios for the NI cyber security sector in its attempt to reach the 5,000 FTE jobs target. We estimate that by 2030, the GVA of the NI cyber security ecosystem could reach up to **£437m per annum** (2.7x current levels).

Over the next decade (2021 – 2030), this would support the **direct cumulative GVA of up to £2.9bn for the NI economy.**

Overall, Northern Ireland is strategically placed, with its wide range of R&D and academic assets and its growing industry expertise. With among the most competitive salaries for cyber security across the UK regions, and established engagement with external investors in the sector, NI has the potential to meet growth ambitions.

Need to ensure a sustainable pipeline of talent:

This research has also undertaken an analysis of recruitment flows into the leading cyber security employers in the region. It demonstrates that there is significant recruitment from broader IT sectors, the graduate pool, other FDI firms, and local firms into top FDI firms. However, indigenous firms can struggle to recruit new talent, and there is a quantifiable shortage of supply within the local ecosystem.

[1] ASHE (2019), median annual salary of £28,000

The DCMS Cyber Recruitment Pool research, alongside the NI jobs target suggests that, whilst there are an estimated c. 100 graduates entering the cyber security sector on average per year – there is a need for at least an additional 300 people to enter the sector each year from other sources.
The recent Assured Skills Academies focusing on cyber security (e.g. Microsoft) and the investment to train up to 1,000 young persons through the Immersive Labs platform offer a good model to encourage pathways into cyber security roles. These should be monitored with respect to employment outcomes and team growth.

Key Recommendations:

Recommendations offered as part of this research to support growth are outlined below, and include:

Pipeline of Talent:

- Support in the development of a sustainable pipeline of talent, including the education and entry of talented high value cyber security professionals, as well as opportunities for career retraining and apprenticeships for those employed in sectors with similar skill sets.

Partnerships and Collaboration:

- Increase of the strength of relationship between academia and private sector, e.g., support the development of joint research projects, research projects with a commercial application, as well as supporting the development of academic spinouts;

Knowledge Sharing:

- Promotion of knowledge sharing in Northern Ireland's cyber security ecosystem, embedding academic staff in industry, and creating channels to allow industry to inform the curriculum of local institutes to meet industry needs;

International Engagement:

- Support in the development and fostering of partnerships with sister cities, that is, relationship building between NI cities and other global cyber hotspots. An example of this includes the growing connection between Belfast and Boston as a result of Rapid7's presence in Northern Ireland;

Complementary Skillset Development and Training:

- Foster AI and ML-related training and technology, supporting the diversification and future-proofing of skillsets in the sector, in turn increasing the resilience of the sector in the region which supports firms in meeting future cyber security needs; and

Promoting the Region:

- Promote NI as the location for commercial R&D in cyber security. NI is home to a strong R&D-focused ecosystem, offering fewer advisory services than the rest of the UK, and more product development services. CSIT should engage partners in the UK, publicising existing R&D activity in NI, and promoting engagement in the region for development needs.

2 Introduction

Context

CSIT was established as the UK's national Innovation & Knowledge Centre (IKC) for cyber security in 2009 and is one of the UK's first Academic Centres of Excellence in Cyber Security Research accredited by the National Cyber Security Centre.

In the last decade, CSIT has developed an extensive research, innovation, policy and teaching offering, and provided an active role in supporting the growth of the NI cyber security cluster. It now has over 70 academic, research, engineering, and professional services staff, which have played a key role in attracting investment, and incubating the thriving NI cyber security ecosystem.

CSIT has commissioned this study with Perspective Economics to identify the current size and scale, and potential of the cyber security ecosystem in Northern Ireland, which at present includes over 100 companies employing almost 2,300 staff.

CSIT recognises the link between its strong research and engineering capabilities, its role as a key generator of cyber security talent, and the leadership shown to attract new investment to Northern Ireland, leading in cyber security research, development and innovation activities in areas of strategic national importance, such as:

- post-quantum cryptography,
- hardware and supply chain security (IoT),
- critical infrastructure (ICS and SCADA),
- cloud and software defined networks (network core),
- mobile malware (Edge),
- AI for cyber, security intelligence and cyber-physical systems.

These areas are essential to national security, but also to ensuring Northern Ireland's cyber security capabilities are world-leading, meet real-world issues, are resilient, and are at the forefront of technological change; allowing Northern Ireland to take best commercial advantage of such opportunities, and promoting high productivity roles in the local economy.

Methodology

Within this research, the team has identified 104 providers of cyber security products and services (aligned to the definition set out within the UK Cyber Security Sectoral Analysis, but also captures key cyber security employers in the region).

Each business has been matched against web data and Companies House registration data (to understand name, description, locations etc). Revenue and employment activity has been identified through use of company accounts, LinkedIn, and or direct engagement with site leads.

The research team has also undertaken analysis of employment and recruitment trends utilising the Burning Glass Technologies and LinkedIn platforms. The key stages are set out below:

Stage 1: Sector Profile

An initial list of 81 firms was provided by CSIT and supplemented with an additional 23 firms identified by a desk review completed by Perspective Economics. This has generated the final list of 104 firms.

The products and services offered within the Northern Ireland cyber security firms were then identified from website descriptions. The final descriptions were used to group firms into six broad service categories, using a 'best-fit' methodology reflecting the main product and service offerings.

The taxonomy was developed to reflect the areas of relative industrial strength in Northern Ireland, and the six final categories include:

- Managed security service provision and advisory services;
- Risk, compliance, and fraud;
- Securing applications, networks and cloud environments;
- Operational technology, security and connected devices;
- Threat intelligence, monitoring, detection and analysis; and
- Identification, authentication, and access control)

A headcount of total employees within the sector was also completed, building on past engagement undertaken by CSIT with firms, as well as the review of publicly available employment figures from LinkedIn profiles.

Stage 2: Economic Profile

An economic profile of the sector was produced based on current offering in Northern Ireland and supplemented with research previously undertaken by Perspective Economics that profiled the size and scale of the UK's cyber security sector, and review of cyber skills in the UK labour market.[2]

This included an estimation of regional GVA related to cyber security in Northern Ireland (estimated using average salary and estimated profit per employee). GVA forecasting up to 2030 is based upon three scenarios, weighted to take account of potential changes in salary and GVA levels, and NI's ambitions to reach the 5,000 jobs target by 2030. The 5,000 FTEs jobs target is considered achievable, and is set out later within this report.

[2] DCMS, Cyber Skills in the UK Labour Market (2020). Available at: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020

3 Sector Profile

The section below provides an overview of the:

- Services on offer from firms engaging in cyber security activity in Northern Ireland;
- Key characteristics of companies operating in the sector, including location, number of firms across taxonomy groups, employment across taxonomy groups, and an overview of key employers; and
- The role of FDI and investment priorities shaping the sector.

Cyber Security Products and Services

The Northern Ireland cyber security ecosystem contains 104 companies offering varied products and service solutions.

The role of CSIT as a world-leading research centre within the region has meant that many of the firms that have invested in Northern Ireland have set up research and development offices in the region. This means that Northern Ireland is home to cyber security providers that are developing new products and services and embedding innovative practice across the globe, and not only providing cyber security services at home.

Within the DCMS Cyber Security Sectoral Analysis exercise, there are ten industrial domains identified within the 'cyber security taxonomy'. However, when defining the sector within Northern Ireland, Perspective Economics reviewed each of the providers and classified them into six key areas considered of strength within the NI ecosystem.

These areas are aligned to Invest NI categories, and were developed to demonstrate the overlap between local cyber capabilities, and use cases across wider sectors (e.g., finance, defence, professional services etc.)

Please note that whilst there are some businesses that cover more than one category, we have assigned each business to a 'best-fit' category, identifying their main product or service and the areas of relative industrial strengths in Northern Ireland.

The table overleaf sets out each of these categories and definitions. Please note these are not exhaustive and are indicative of the main product or service offered in each.

Table 3:1 Cyber sector taxonomy definitions

Category	Definition
Managed security service provision and advisory services	This refers to firms typically selling cyber security services to an external party, primarily focused on outsourced cyber security. For example, where a business procures an MSSP to undertake cyber security monitoring, network security, patching and remote device management, penetration testing, and broader security and IT advice.

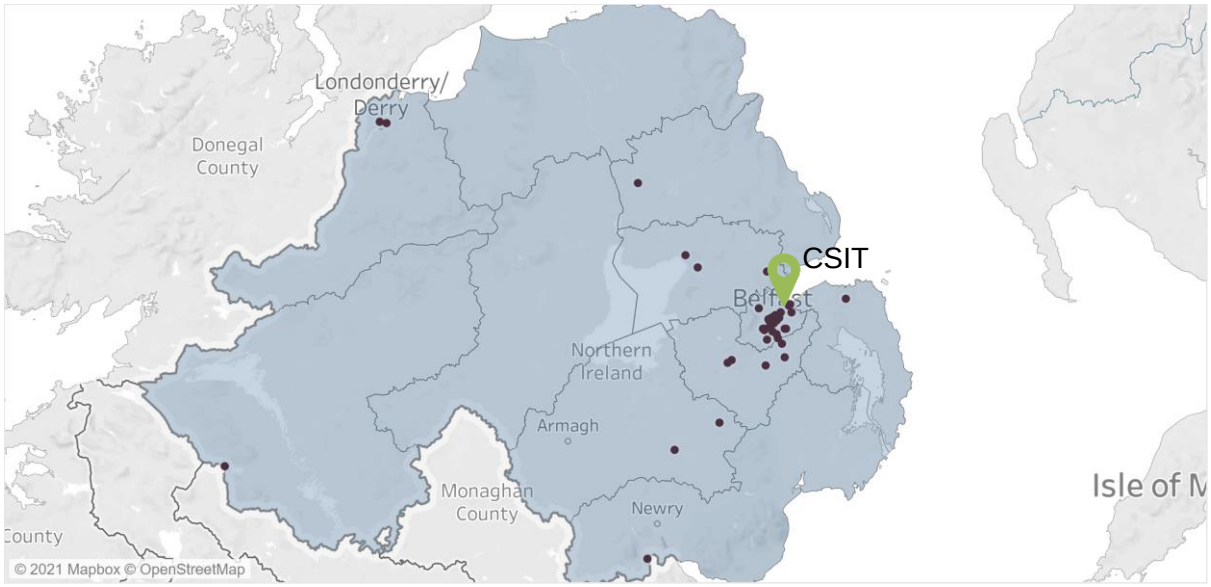
Risk, compliance, and fraud	This refers to firms where the focus of cyber security techniques is upon identifying risk (such as harmful actors or anomalies), ensuring compliance with cyber security standards (e.g. ISO27001 and GDPR) with respect to data management, and identifying and mitigating fraud within transactions. There is strong overlap between this field, and Fintech / payment processing.
Securing applications, networks and cloud environments	This refers to firms that develop or implement products or solutions with respect to application security, networks or cloud infrastructure. This might include identifying and patching potential software or network exploits, or applying secure parameters to network or cloud environments e.g. ensuring infrastructure is encrypted, ensures DLP, and has appropriate authentication / user controls in place.
Operational technology, security and connected devices	This refers to the manufacture and distribution of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.
Threat intelligence, monitoring, detection and analysis	Refers to 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.
Identification, authentication, and access control	Refers to firms offering systems designed to support the verification of users accessing systems.

Source: CSIT, Perspective Economics

Number and Location of Cyber Security Companies

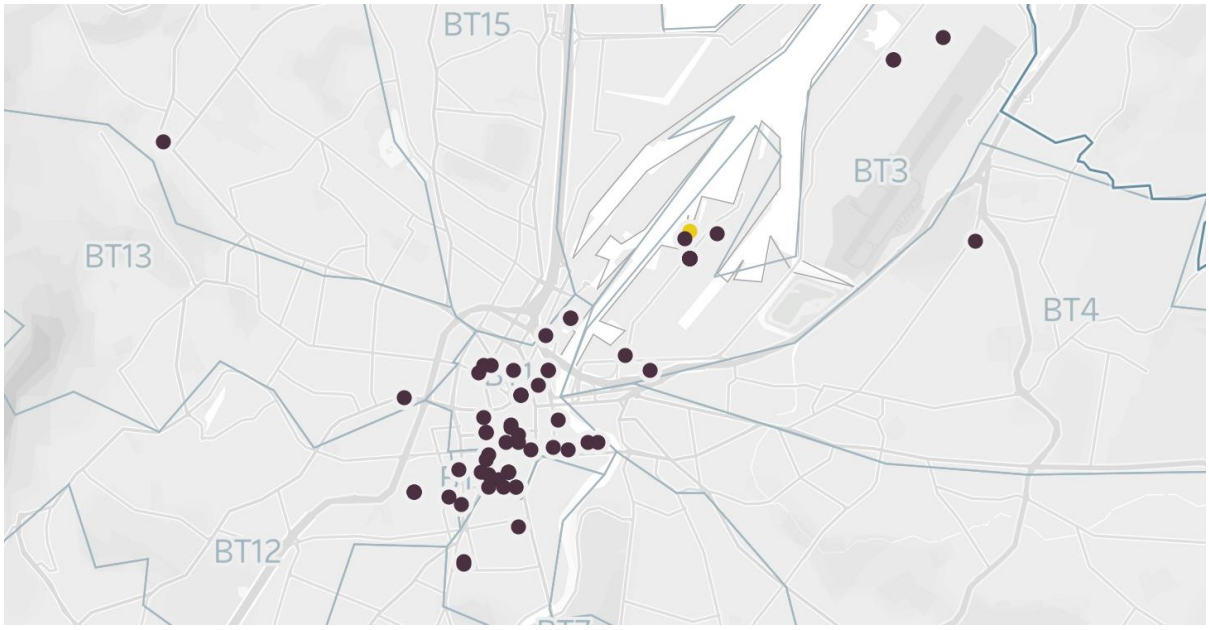
There are currently 104 firms working in the cyber security sector across Northern Ireland. The locations of cyber security firms operating in NI are detailed in the figure below:

Figure 3:1 Location of NI cyber firms



Source: CSIT, Perspective Economics

Figure 3:2 Location of Belfast cyber firms



Source: CSIT, Perspective Economics

The Belfast city area is home to 84% of all NI cyber firms, which highlights the city's status as a UK cyber hub with emerging tech specialisms, ranked 2nd in the UK, and 9th globally within the Top 25 Tech Cities of the Future 2020/21.[3]

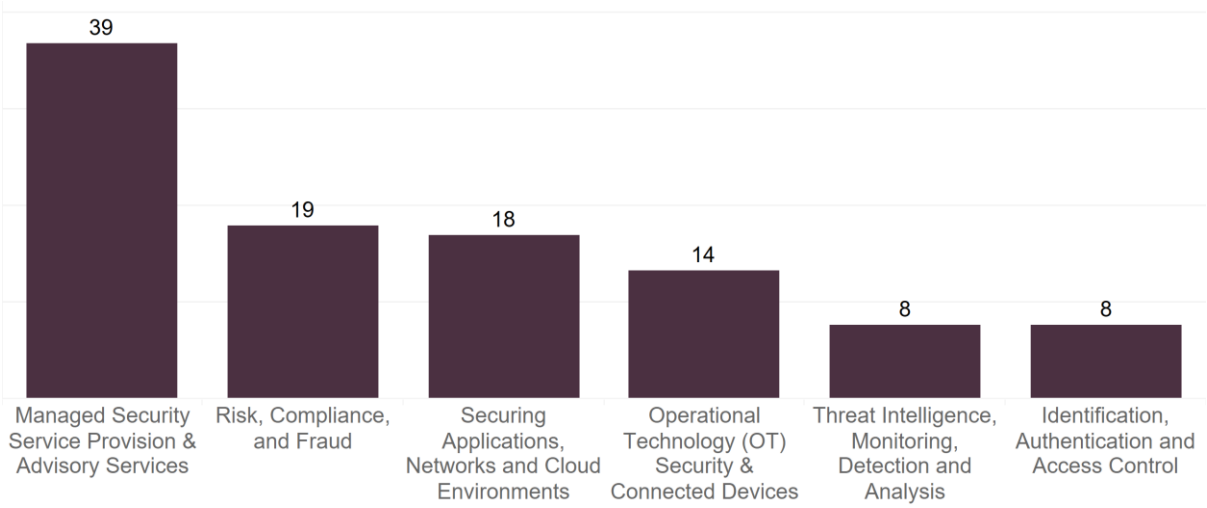
[3] Global Outlook Tech Cities of the Future 2020/21

Assets within the region make it an ideal location for cyber firms. These include:

- The growing graduate market from Queen's University and University of Ulster (specific courses include a PhD in Cyber Security, MSc in Applied Cyber Security, Higher Level Apprenticeship in Cyber Security and Networking Infrastructure, Postgraduate Certificate in Cyber Security);
- Alternative entry and training through Belfast Metropolitan's cyber academy, which offers a bespoke programme and skills training to support a growing business, developed in conjunction with the Department for the Economy Assured Skills programme and Invest NI, as well as industry;
- Microsoft's Skill Academy for graduates with a 2:2 degree classification or a level 5 qualification in an IT-related subject;
- OWASP Belfast, which is Ireland's largest chapter producing freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security;
- Partnerships between CSIT and Deloitte in delivering LORCA (the London Office for Rapid Cybersecurity Advancement); and
- Additional CSIT projects such as RISE, the UK's Hardware Security Institute which is one of four cyber security institutes in the UK and will be a global hub for research and innovation in hardware security.

The figure below provides an overview of total number of firms operating in each of the 6 taxonomy groups.

Figure 3:3 Firm Classification



Source: DCMS, Perspective Economics

Overall, within the Northern Ireland cyber security sector, we have segmented each of the firms into a considered 'best-fit' classification to understand the strengths of the local ecosystem. The following number of firms focus on:

- 39 firms offering Managed Security Service Provision and Advisory Services, including firms such as Cyphra, Ansec IA, and Fujitsu.
- 19 firms focus on solutions with respect to Risk, Compliance, and Fraud. This includes firms such as Metacompliance, Aflac, Cybersource NI, Allstate and Citi.

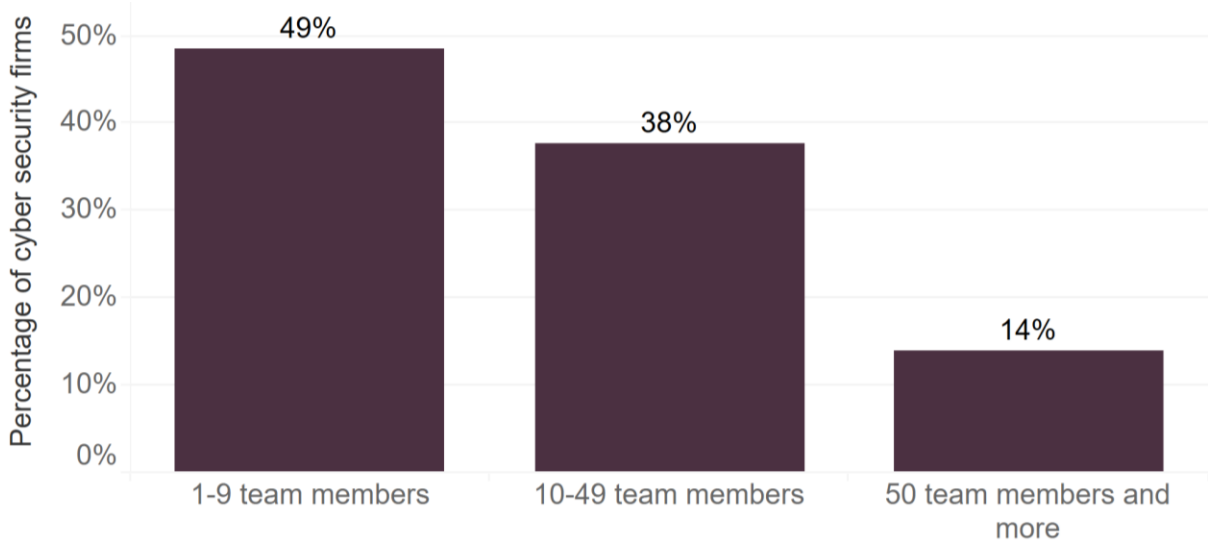
- 18 firms are engaged in Securing Applications, Networks and Cloud Environments solutions. The largest of these include Rapid7 and Whitehat Security.
- 14 firms focus on Operational Technology, Security and Connected Devices, including firms such as NVIDIA, Kigen and Angoka, and Seven Technologies Group.
- 8 firms are engaged in Threat Intelligence, Monitoring, Detection and Analysis, including firms such as Proofpoint, Imperva and Anomali.
- 8 firms are also engaged in Identification, Authentication and Access Control services, examples including B-Secur, SaltVPN and Liopa.

It should be noted that the sectoral overview presented above offers insight into the number of firms currently operating in Northern Ireland across each taxonomy group. This analysis is completed again below, offering a more accurate view of workforce capacity across each of the taxonomy groups.

Number of Employees in the NI Cyber Security Sector

There are an estimated 2,299 cyber security employees currently within Northern Ireland's cyber sector (i.e. across the 104 private firms). This figure below details the size of **cyber teams** across these identified firms:

Figure 3:4 Company size // Cyber security employees



Source: CSIT, Perspective Economics

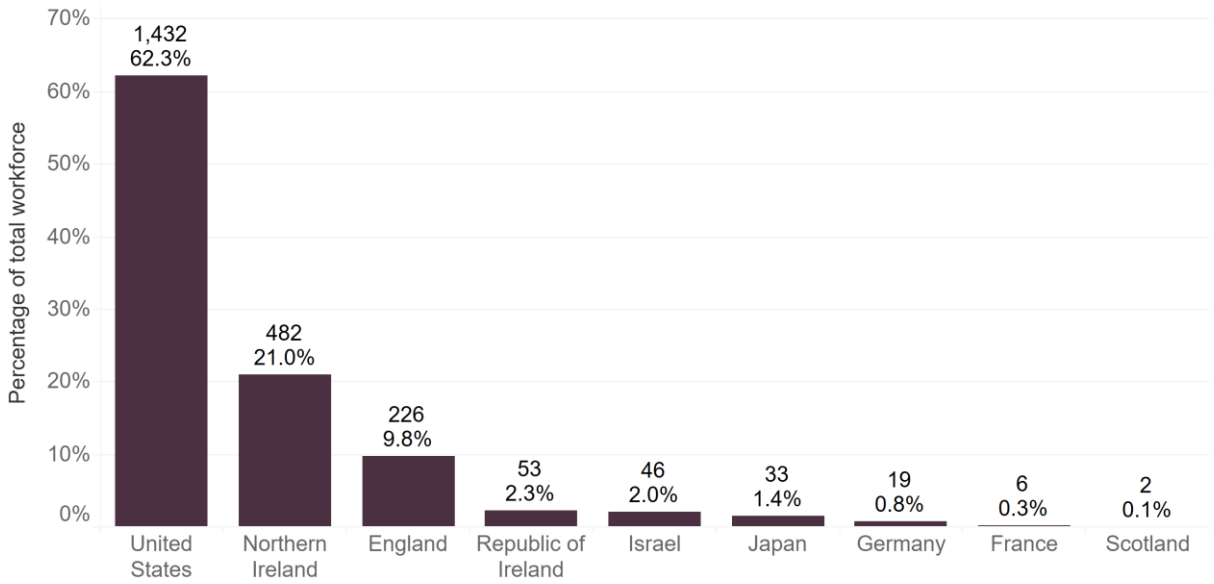
The figure shows that typically, of the 104 NI-based cyber security teams within firms are small, suggesting that:

- Almost half (49%) of all cyber teams contain fewer than ten employees;
- 38% of firms have cyber teams of between ten and fifty employees; and
- 14% have teams with fifty or more staff working in cyber security roles.

Foreign Direct Investment (FDI) has also played an important role in shaping the NI cyber sector. This is most notable when exploring the breakdown of employment in the NI cyber security ecosystem by country of origin.

The figure below sets out the extent to which employment in NI is FDI-driven:

Figure 3:5 Percentage of employees by country of origin



Source: Perspective Economics

In total, nearly four in five (79%) jobs in the NI cyber security sector are supported by firms headquartered outside of Northern Ireland.

Further, firms from the United States are among the strongest employers for cyber security talent in the region, employing 62% of the workforce. This includes firms such as Allstate, Citi, Aflac, Proofpoint, Rapid7 and Anomali.

This is a significant finding, as this employment has the potential to support skills development, enable enhanced investments in the region (where Northern Ireland is recognised as a global hotspot for cyber security talent), and to enable positive spillover across the wider ecosystem (e.g. where new start-ups can be formed and grown locally).

Further, it also helps to connect NI's workforce and academic community with industry leaders at a global level.

Some of the key employers within the sector are outlined in the table below. Key employers include US-based Rapid7, Allstate, and Proofpoint, GB headquartered PwC and ARM (Kigen), and NI firms Metacompliance, Novosco and B-Secur.

Table 3:2 Notable employers

Taxonomy Group	Example Employers (as of April 2021)
Securing Applications, Networks and Cloud Environments	• Rapid7, IBM, Whitehat Security
Risk, Compliance and Fraud	• Allstate, Metacompliance, Cybersource
Threat Intelligence, Monitoring, Detection and Analysis	• Proofpoint, Anomali, Imperva

Managed Security Service Provision and Advisory Services	• Novosco, PwC, Fujitsu
Operational Technology Security and Connected Devices	• ARM (Kigen), Johnson Controls, Sensata Technologies
Identification, Authentication and Access Control	• Anyvision, B-Secur, Core Systems NI

The role of Foreign Direct Investment

As set out previously, Foreign Direct Investment has played a key role in growing the sector. This is also reflected in the company data, which highlights more than a third (36%) of cyber security firms in the region are headquartered in the United States, and almost a fifth (17%) elsewhere in the UK.

However, 38% of firms are indigenous to the region, which also highlights that Northern Ireland has a strong base of local firms that offer considerable growth and investment opportunities for the region.

Table 3:3 Headquarters location

Headquarter Location	Total number of firms
Northern Ireland	39 (38%)
United States	37 (36%)
England	17 (16%)
Republic of Ireland	3 (3%)
France	3 (3%)
Japan	2 (2%)
Scotland	1 (1%)
Israel	1 (1%)
Germany	1 (1%)

Source: Perspective Economics

The strong presence of foreign owned business places NI's cyber security sector strategically within a wider global network, supporting exposure and engagement with firms headquartered in the United States, Great Britain, the Republic of Ireland, and further afield.

Perspective Economics has reviewed Invest NI Financial Offers of Support (2015 – 2020) to identify financial assistance made to cyber security firms in the region by Invest NI for job creation. We have identified, in total, Invest NI has provided c. £27m worth of financial support between 2015 and 2020 to the sector (to help stimulate £170m of private investment). This funding has supported the creation of more than 1,300 jobs.

Sector Summary

The table below offers a summary of firms and employees across taxonomy groups, offering insight into the average team size, and once again highlighting the role of FDI in supporting employment, with increase in average team size correlating with the percentage of firms headquartered outside NI.

Table 3:4 Employment across taxonomy categories

Taxonomy Group	Number of firms	Number of cyber employees	Average size of cyber security team
Securing Applications, Networks and Cloud Environments	18 *(17%)*	637 *(28%)*	35
Risk, Compliance and Fraud	19 *(18%)*	602 *(26%)*	32
Threat Intelligence, Monitoring, Detection and Analysis	8 *(8%)*	438 *(19%)*	55
Managed Security Service Provision and Advisory Services	37 *(36%)*	250 *(11%)*	7
Operation Technology Security and Connected Devices	14 *(13%)*	215 *(9%)*	15
Identification, Authentication and Access Control	8 *(8%)*	157 *(7%)*	20

Source: Perspective Economics, CSIT

4 Economic Profile and Potential

The section below provides an overview of the economic profile and potential of Northern Ireland's cyber security sector. This includes:

- The role of the region's cyber security sector in light of Northern Ireland Executive policy;
- A review of current salary within the sector;
- Benchmarking of salary and demand against other UK regions;
- Growth ambitions in the region; and
- Suggested targets and actions.

Cyber Security within the NI Economy

The importance of growth in the sector is recognised in Northern Ireland Executive's Economic Recovery Action Plan and the New Decade, New Approach deal.

This deal sets out commitments to promote Northern Ireland as a global cyber security hub, recognising and building on NI's *"blend of world-class talent, leading forensic science expertise and tech research excellence"*, to achieve 5,000 cyber security job roles by 2030.

This is emphasised in NI's Cyber Security Strategic Framework for Action (2017-2021), which acknowledges the need to diversify the economy in NI to support growth, while also highlighting the need to access new markets as well as new forms of wealth creation, and again in the Economic Recovery Action Plan, which highlights ambitions to offer free online access to skilled training within a cyber security job vacancy platform.

The framework suggests that cyber security will not only play a role in creating jobs but will also promote NI as a location for digital technologies, attracting firms to NI with its existing skill market in cyber security.

To meet the ambitions set out to support the NI economy, the framework highlights current needs within the sector, such as addressing skills shortages, which involves engagement between public and private sector alongside academia.

Other priorities set out within the framework include the need to capitalise on opportunities to secure investment and growth in the cyber sector and research; more effective law enforcement to deter future threats and criminal activity; and increased activity to build public trust in public services.

In terms of current GVA, the NI cyber sector is estimated to currently generate c. £161m (2021) each year.

By 2030, we estimate that the sector could generate c. £437m in GVA, resulting in £2.9bn in cumulative GVA generated by the cyber sector in Northern Ireland over the next decade.

Salaries and Productivity

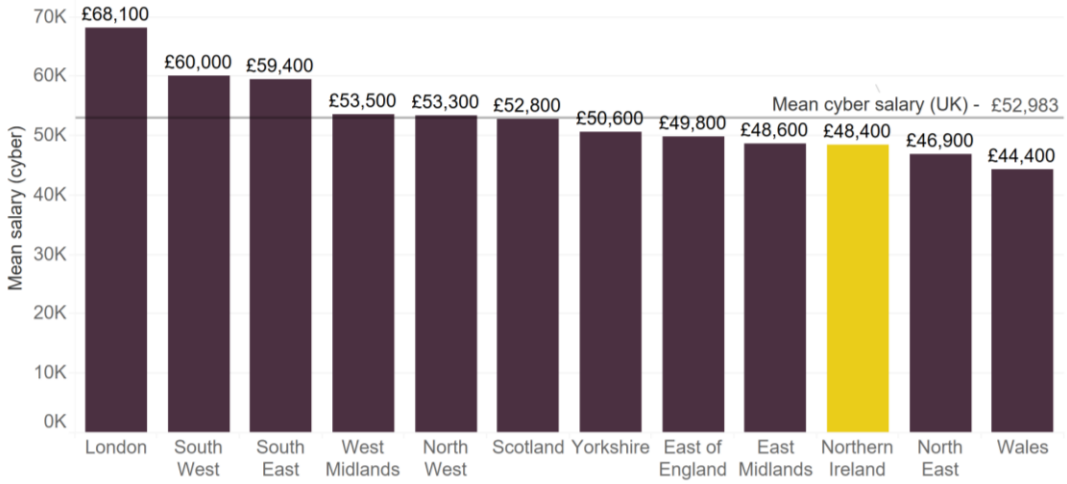
The average advertised salary for a cyber security employee working in Northern Ireland is estimated (2020) at £48,400 per annum, as set out within the DCMS UK Cyber Skills in the Labour Market Report (2021)[4].

Based on current employment levels (2,299), total salaries across the cyber security sector are estimated at £111.3m.

There are three key advantages of Northern Ireland pursing cyber security as a key sector to increase regional productivity.

- Firstly, salaries in cyber security in Northern Ireland are significantly above those experienced in the wider Northern Ireland economy. In 2020, median annual earnings for full-time employees in Northern Ireland reached £28,000 (below UK median of £31,000) (ASHE: 2020[5]). This suggests a significant wage premium associated with cyber security roles compared to the wider economy (particularly private sector roles).
- Secondly, whilst the average salary level for Northern Ireland cyber security roles is much higher than other sectors; it remains attractive within a UK (i.e., 18% lower than the UK average of £59,200, and almost 30% lower than the London average of £68,000) and international context.

Figure 4:1 Average Advertised Salary (by Region) for Core Cyber Roles



Source: Burning Glass Technologies (n = 55,032)

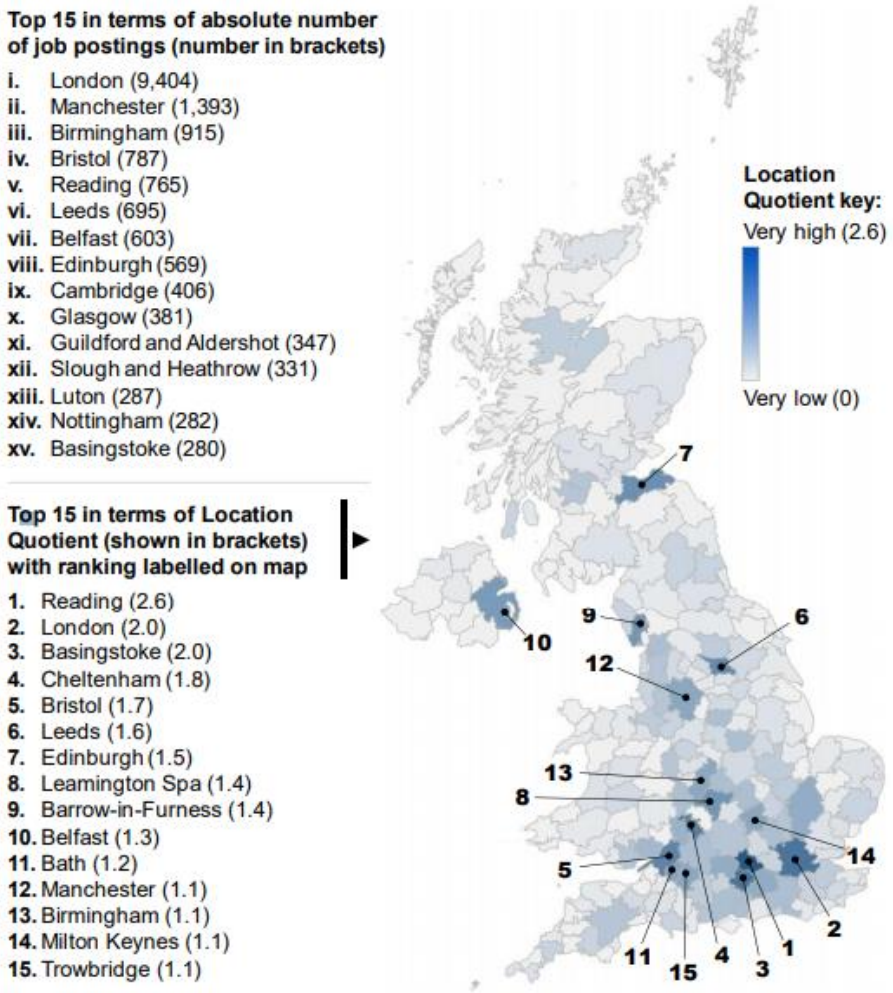
- Thirdly, the density of international investment in cyber security within the region means that there is an interest in training initiatives to bring new talent into entry-level cyber security roles e.g. in incident response and vulnerability analyst roles. This offers Northern Ireland a unique opportunity to retrain and upskill people into cyber security at scale, and should provide opportunities for entrants to increase their earning potential particularly in the medium and long-run – thereby helping to increase longer

[4] DCMS (2021) Cyber Security Skills in the UK Labour Market: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021
[5] ASHE (2020) https://www.nisra.gov.uk/news/annual-survey-hours-and-earnings-2020#:~:text=Median%20annual%20earnings%20increased%20by,approximately%20%C2%A352%2C000%20and%20above.

term productivity. For example, it is not uncommon for individuals with excess of five years' experience to earn over £70,000 per annum.

Recognising the skills, support available, and the competitiveness of the region, it is clear that employers are interested in expanding cyber security operations within Northern Ireland. This is emphasised in the figure below, which shows that the relative level of demand (measured by number of job postings) in the Belfast region is among the highest in the UK.

Figure 4:2 Regional Demand for Cyber Talent



Source: Burning Glass Technologies (n = 24,759 core cyber job postings from January to December 2020 where TTWA was listed (out of a total 33,622)

Growth Ambitions

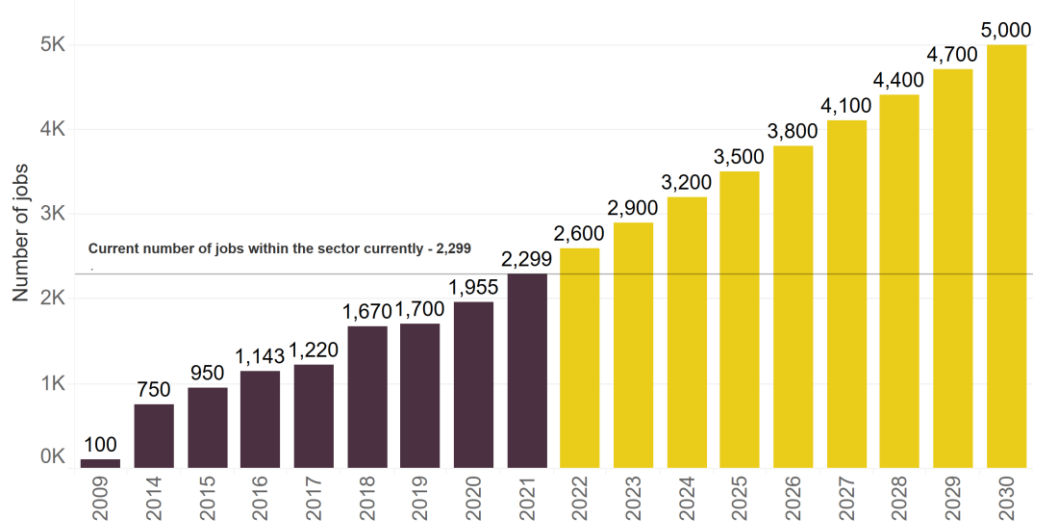
As set out previously, there is an ambitious jobs target in place for the Northern Ireland cyber security ecosystem of 5,000 FTE roles in place by 2030. The current employment estimates indicate that the sector is almost halfway to the 2030 target. In order to meet this jobs target by 2030, the sector must grow (net) by approximately 300 employees per year up to 2030.

Whilst this is considered achievable (for example, the sector has grown by approximately 350 people in the last twelve months), workforce modelling is required to understand the flows of where new talent is coming from (e.g. new graduates, conversion / training, or movement of people from other IT firms (locally and externally) into NI cyber security roles).

Research into the UK's Cyber Security Recruitment Pool (2021)[6] highlights that the UK needs to train at least 10,000 new people each year into cyber security to keep up with expanding demand, and meet industry supply requirements.

Weighting this figure to Northern Ireland suggests that, in addition to more than a hundred graduates entering cyber security roles each year, the region **should explore opportunities to develop approximately two to three hundred additional people in cyber security each year**. This could take the form of increasing university places (where practical or possible), increasing access to further education and apprenticeship routes into cyber security, encouraging accessible retraining, and continuing to fund initiatives such as the Assured Skills Academies.

Figure 4:3 Required yearly growth



Source: CSIT, Perspective Economics

GVA Growth Scenarios

Average salaries and estimated profit per employee was used to estimate GVA against the NI growth ambitions for the cyber security sector. The data suggests that GVA per cyber security employee is approximately £70,000, based on current salary (£48,400), and calculated profit (£21,600). This is consistent with the estimated GVA per cyber security employee at the UK level (£85,700) as set out within the UK Cyber Security Sectoral Analysis.

From this, current and potential GVA from the sector by 2030 was calculated. This is outlined overleaf across three scenarios which provide an estimation of sector GVA if:

i) GVA per employee increases 2.5% per year, and Northern Ireland reaches the 5,000 jobs;
ii) GVA per employee remains level, but the 5,000 jobs target is met; and

[6] DCMS (2021) Understanding the UK Cyber Recruitment Pool: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973914/Ipsos_MORI_Cyber_Recruitment_Report_v1.pdf

iii) GVA per employee increases 2.5% per year, but the sector fails to meet the full jobs target.

Within the above scenario, salary increase is based on the average change in advertised salaries identified between 2015 and 2019 through the Burning Glass platform.

Scenario 1: salaries increase 2.5% per year, and job targets are met

Year	GVA per employee	Job target	GVA
2021	£70,000	2,299	£160,930,000
2030	£87,420	5,000	£437,102,039
		Cumulative (2021-2030):	**£2,910,272,934**

Scenario 2: GVA per employee remains level (in current terms), but job targets are met

Year	GVA per employee	Job target	GVA
2021	£70,000	2,299	£160,930,000
2030	£70,000	5,000	£350,000,000
		Cumulative:	**£2,554,930,000**

Scenario 3: salaries increase 2.5% per year, but the sector fails to meet growth targets

Year	GVA per employee	Job target	GVA
2021	£70,000	2,299	£160,930,000
2030	£87,420	3,567	£311,785,197
		Cumulative:	**£2,290,214,006**

If the cyber sector achieves the targeted number of employees, and the average salary increases 2.5% per year in line with expectations, by 2030 the sector will have an estimated GVA of £437m per annum (and will have added £2.9bn of GVA to the NI economy over the full decade).

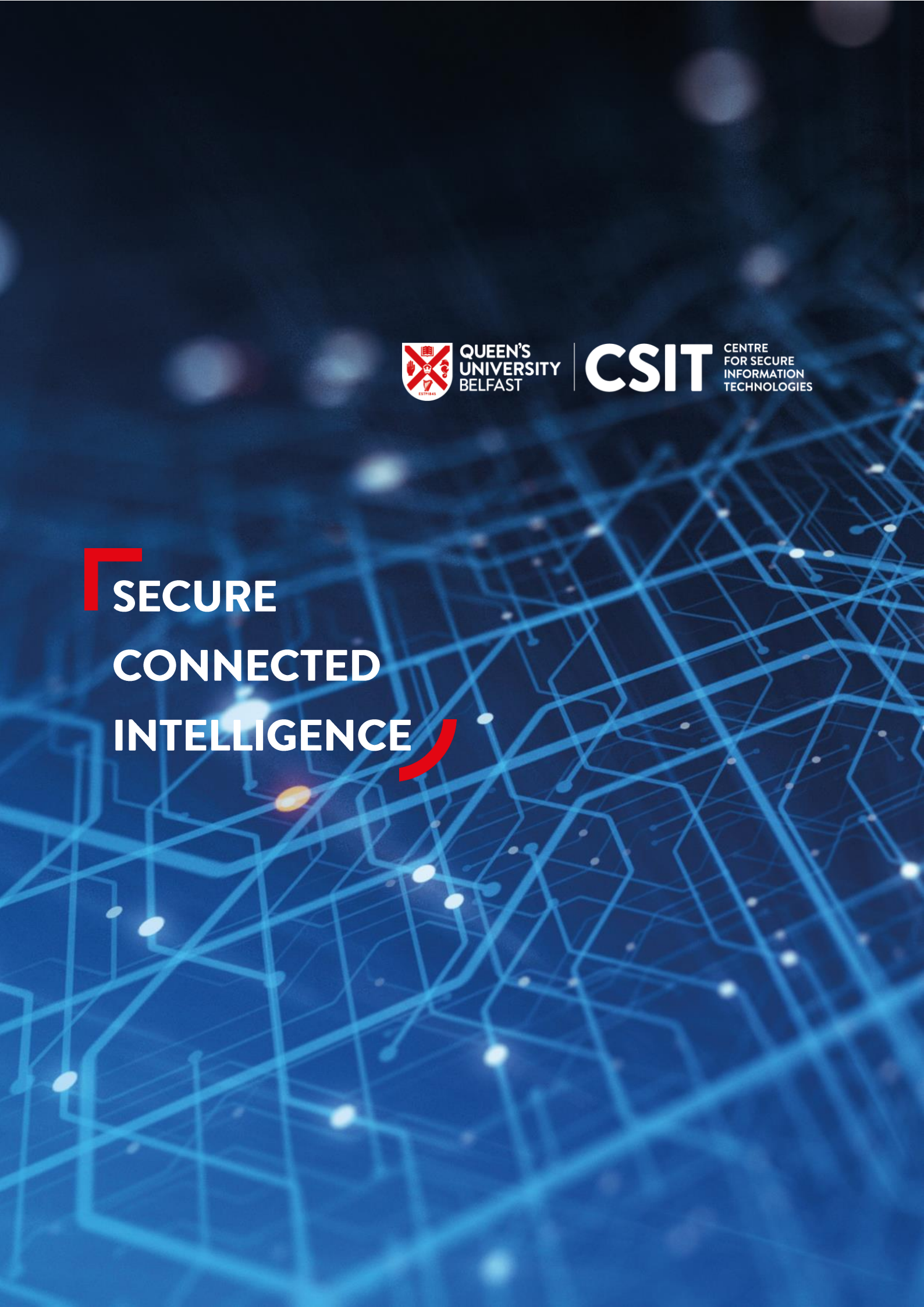
This illustrates the need to promote entry into cyber security roles and ensure sustainable employment growth to meet the targets set out by the Northern Ireland Executive. On this basis, investments in initiatives to grow the local ecosystem, such as funding for research and development and engineering (to promote high value projects and grow teams around new technologies), attracting new investment, and increasing the skills pipeline would be particularly welcome.

Suggested Actions

Based on the review of the Northern Ireland's cyber sector's economic profile, and the ambitions set out by Northern Ireland Executive, there are a number of ways for local partners to further support sustainable development and job growth in the sector and contribute to the fulfilment of the 5,000 cyber roles by 2030.

Proposed actions to support growth should include:

- Support the development of a sustainable pipeline of talent, including the education and entry of talented high value cyber security professionals, as well as opportunities for career retraining and apprenticeships for those employed in sectors with similar skill sets.
- Increase the strength of relationship between academia and private sector, e.g., support the development of joint research projects, research projects with a commercial application, as well as supporting the development of academic spinouts.
- Promote knowledge sharing in Northern Ireland's cyber security ecosystem, embedding academic staff in industry, and creating channels to allow industry to inform the curriculum of local institutes to meet industry needs.
- Support the development and fostering of partnerships with sister cities, that is, relationship building between NI cities and other global cyber hotspots. An example of this includes the growing connection between Belfast and Boston as a result of Rapid7's presence in Northern Ireland.
- Foster AI and ML-related training and technology, supporting the diversification and future-proofing of skillsets in the sector, in turn increasing the resilience of the sector in the region which supports firms in meeting future cyber security needs.
- Promote NI as the location for commercial R&D in cyber security. NI is home to a strong R&D-focused ecosystem, offering fewer advisory services than the rest of the UK, and more product development services. CSIT should engage partners in the UK, publicising existing R&D activity in NI, and promoting engagement in the region for development needs.


QUEEN'S UNIVERSITY BELFAST
CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES
SECURE
CONNECTED
INTELLIGENCE