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

perspective economics

DECEMBER 2025

# Northern Ireland Cyber Security Snapshot: Summary Report

## 2025 Update

# 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. The 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.

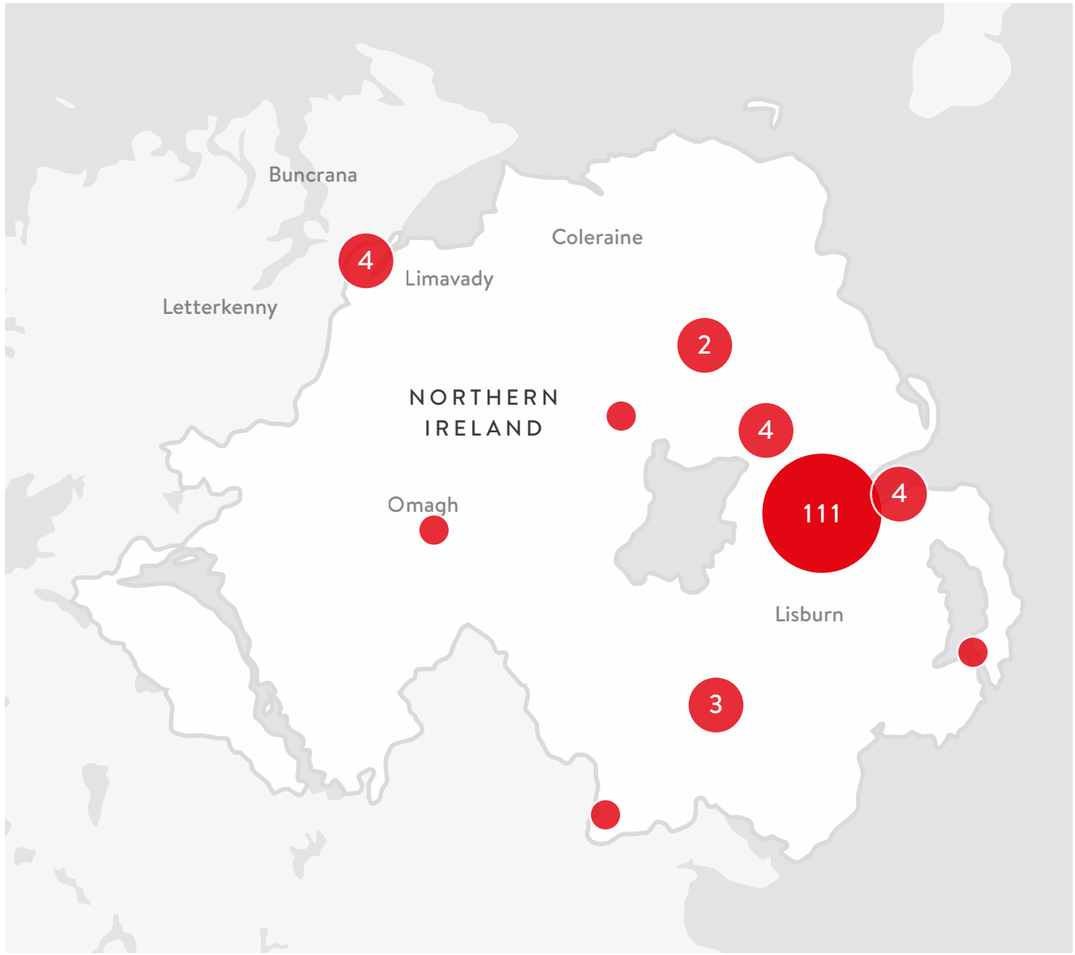
Despite these challenges, there is an underlying depth in expertise, research activity, and new commercial domains in cyber security that Northern Ireland
can best exploit. As such, this report provides an assessment of core challenges and opportunities in the years ahead, to ensure that Northern Ireland's 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

# 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.

## 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.

## 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.

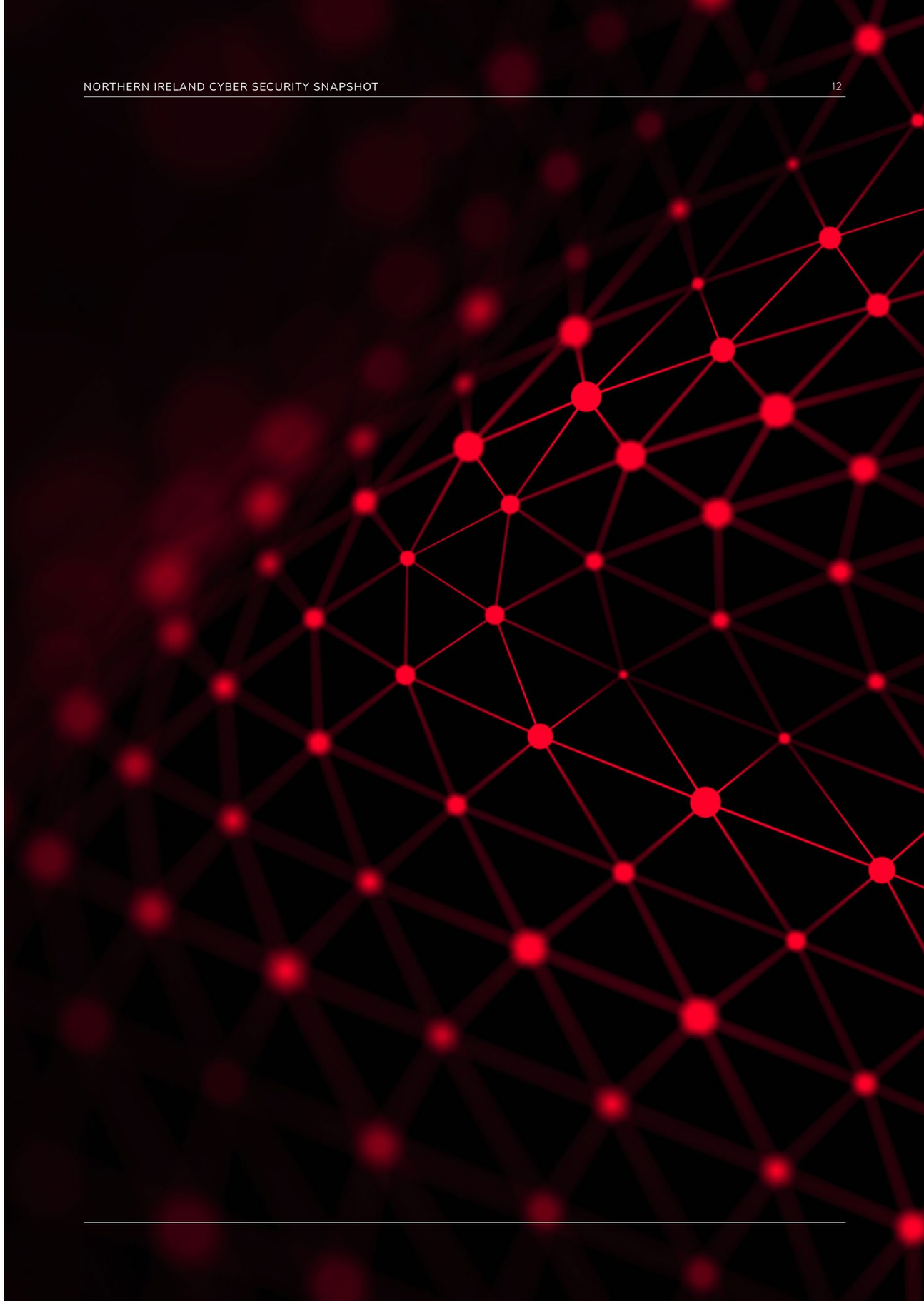
- Expand collaborative research programmes that connect academic expertise with industry challenges, ensuring that research outputs are designed with bleeding-edge technical development or commercial applications in mind.

- 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/