1. Company Details

Legal Status:	Private Limited Company
Business Name:	CyberSpark Group Ltd
Address:	248 Upper Newtownards Road, Belfast BT4 3EU
Tel:	03332 244731

1.a Company Background

CyberSpark Group has been registered as a Limited Company since 2017 and is designed to deliver training in a broad range of cyber skills to young people in Northern Ireland.

CyberSpark Academy has been established as the main vehicle for CyberSpark NI Group's strategy to deliver a training and educational pathway for cyber security training and provide young people with a better understanding of IT foundational skills.

CyberSpark Academy has contractual links with several Cyber Companies and Certifying Bodies to deliver cyber training and education to Commercial and Government Organisations as well and delivering training in schools. The Academy has the support of PA Consulting, Nihon Cyber Defence (NCD), SALTVPN and its Certifying Body is (ISC)². (ISC)² will certify students of the Academy from the basic introductory level to professional qualifications through the Certified Information Systems Cybersecurity Certification (CISSP).

2. Activities

The Academy will deliver a range of courses listed at paragraph 3a as well as introductory Micro:bit introductory courses in primary schools.

2. a Training and Education

The Academy has entered into a partnership with (ISC)² to provide commercially recognised Qualifications in Cyber and IT through the Academy conducting classroom led training and mentoring in different facets of the Cyber and IT spectrum. The Academy has enlisted Cyber Professionals to provide the lessons, whilst the Academy's Managing Director holds qualifications in relation to security investigations including the Laws concerning Privacy and ECHR, Data protection and RIPA. The Directors of the Academy have also been involved in the mentoring of Adult Transitioning Programmes to enable them to find suitable work and job placement ~~and~~ together with ongoing mentoring to assist in their transition, as well as providing education to Children aged 10 years and upwards whilst in education.

The mentoring for ~~the~~ Children and Young Adults is for the "hard to reach" in Society and those who come from troubled or deprived backgrounds, which has seen major success in the placement of such Young Adults into IT based jobs with an 80% success rate. CyberSpark ran a pilot Coding Course in a local Primary School and, following its success in the presence of the Minister for Education has had discussions at Ministerial level~~s~~ to introduce curricular support for teachers of IT and Coding at Secondary School level. The Academy is also engaging with the Youth Justice Agency to provide a Cyber Certificated Course for several Youth Justice groups

2. b Training Cyber Security and IT Infrastructure

Contracts have been put in place and a stratagem devised to deliver cyber training and mentoring. The Academy is in discussion with a number of potential Clients to move forward in the first quarter of 2023. This will assist in meeting Industry and Government requirements, as currently in the United Kingdom there are 2,000,000 IT and Cyber related vacancies, which is detrimental to the UK and Ireland Cyber Infrastructure and Resilience Planning. See:

https://www.bbc.co.uk/news/technology-62098767

The Academy is actively seeking to engage other stakeholders in the Cyber Security Industry in order to enter into contracts with them, with the aim of training Young Adults and Children in Cyber Awareness skills to prepare them for employment in Commercial or Governmental positions. 4Securitas, Meptagon, and Edgescan are some of the Companies that have entered discussions with the Academy for this need.

https://meptagon.com https://4securitas.com https://www.edgescan.com

3. Assessment of Current Products / Services

3. a Training Facilitation Global

There is an obvious omission in the delivery of cyber training in Schools. Everyone is aware of the threat from foreign State sponsored operatives and cyber criminals who wish to damage IT networks or extort funds from organisations or individuals, but very little training is offered in Schools. Naturally the focus is upon guiding students away from sites that promote self-harm, cyber bullying, and harmful content, but there is nothing in the School Curriculum that promotes understanding of cyber security for children in primary or secondary education.

At the same time, there are clear gaps in the ranks of skilled IT professionals, and these are likely to remain until parents have a better understanding of the career opportunities that await those with strong IT skills. At present there are insufficient numbers of qualified staff coming forward to meet the demands of Industry, Commerce, and Government. Unless steps are taken to identify and train students at a much younger age than at present, the situation will deteriorate.

Whilst the focus is on the initiation of the introductory training of cyber skills in primary schools in a small area of Northern Ireland, the plan is to develop and deliver a training package which can be rolled out across the UK and Ireland. There will be two main benefits of this approach. Firstly, the programme can be tailored and developed so that it can be delivered collaboratively alongside School staff in order to give all children a broad awareness of how to incorporate cyber security into their online activities whether it be for School, social or wider engagement. Secondly, some children will display significant aptitude for this training, and this will allow Schools to direct them to further training at the CyberSpark Academy with a view to a career in IT.

We believe that several of the International Companies that have a presence in Ireland are in urgent need of young people with strong cyber skills and would be prepared to offer apprenticeships based upon time at the Academy and work placement. Similar apprenticeships are proving popular in Northern Ireland such as the BrightStart scheme offered by Deloitte.

Beyond Schools, the Academy will seek to engage with individuals who may have found it difficult to secure meaningful employment, including those in the Criminal Justice System, individuals who have dropped out of university or those who have had a career in the Police and the Armed Forces and who are now seeking to return to civilian life. The Academy will offer a range of Certified Courses in order to increase the pool of cyber qualified individuals available to Companies already established in Ireland and as well as helping to attract further investors to come to the island.

The lack of cyber skills training available to young people in education means that there is no effective filter for those seeking to undertake Degrees at the Centre for Secure Information Technology (CSIT) at Queen's University. The Courses delivered by the Academy would provide the foundation for better academic achievement at University as well as practical skills which would help secure immediate employment and career progression in the workplace.

We have engaged with an Organisation which is affiliated to the American Higher Education System and the Reserve Officer Training Corps Alumni and has some 300 Colleges and Universities aligned to their programmes. We are working with our partners to fully engage with the American market in order to train individuals in cyber skills.

This Project has the potential to attract further foreign inward investment and help diversify the skills offered in the UK by attracting those individuals to work in Northern Ireland. This training can be offered at a far more competitive price than similar training in the USA, whilst early indications are that some 1000 students and veterans will come each year. The unique attraction of Ireland to an American audience should not be underestimated.

We, the Directors of CyberSpark, have also made contact with several International Companies who have bought into the ethos of the CyberSpark Group vision and the CyberSpark Academy approach. There is also considerable interest in cyber training from across UK and Ireland Government Departments who have recognised the potential vulnerabilities of their Networks and how their staff can be better prepared to combat attacks.

In order to deliver the relevant training, we have partnered with a globally recognised cyber training and qualifying body to help service the demand for the academy. $(ISC)^2$ will deliver several Commercial Grade

Cyber courses and a Training Agreement has been entered into with them. The Courses will be specifically tailored to meet the needs of Schools in Northern Ireland.

The CyberSpark Academy is developing a 2-day “Introduction to Cyber Security” for Government Departments and private Companies. Cyberspark group are currently negotiating such a package for several groups and are rolling out pilot programmes in first quarter 2023.

The list of (ISC)² courses on offer is as follows:

Certified in Cybersecurity Entry-Level Certification (CICEC) 2 days.

Certified Information Systems Security Professional (CISSP) 6 days.

Certified Cloud Security Professional (CCSP) 6 days.

Certified Authorisation Professional (CAP) 3 days.

Certified Secure Software Lifecycle Professional (CSSLP) 6 days.

HealthCare Information Security and Privacy Practitioner (HCISSP) 3 days.

Systems Security Certified Practitioner (SSCP) 5 days.

	Course Content	Focus	Delivery
CICEC	16 hours of live instruction. Peer discussions. Pre-and post-course assessments. End-of-chapter study sheets and quizzes. Online interactive flash cards. Exam voucher.	Domain 1: Security Principles. Domain 2: Business Continuity (BC), Disaster Recovery (DR), & Incident Response Concepts. Domain 3: Access Controls Concepts. Domain 4: Network Security. Domain 5: Security Operations.	Classroom based, 2-day delivery. No prior experience necessary.
CISSP	Instruction from an (ISC)² Authorized Instructor. Official (ISC)² Student Training Guide. Interactive flash cards to reinforce learning. An applied scenario with 9 corresponding activities teaching you how to apply security concepts to a situation that CISSPs likely encounter in the workplace. 8 discussions encouraging peer to peer interaction around key topics. 71 content specific activities including 6 case studies. 9 end of chapter quizzes with answer explanation to assess comprehension. 180 question post course assessment with answer explanation highlighting areas for further study.	Security Consultant. Security Manager, IT Director/Manager. Security Auditor. Security Architect. Security Analyst. Security Systems Engineer. Chief Information Security Officer. Security Director. Network Architect.	Classroom based 40 hours classroom based. CPD required. Experienced professionals (5yrs).
CCSP	Instruction from an (ISC)² Authorized Instructor. Official (ISC)2 Student Training Guide. Chapter quizzes. Interactive flash cards to reinforce learning. Real-world learning activities and scenarios. Case studies and discussions. Post-course assessment questions to gauge exam readiness.	Security Manager. Systems Architect. Systems Engineer. Security Architect. Security Consultant. Security Engineer. Enterprise Architect. Security Administrator.	Classroom based 40 hours classroom based. CPD required. Experienced professionals (3yr).
CAP	Instruction from an (ISC)² Authorized Instructor. Official (ISC)² Student Training Guide. Chapter quizzes. Interactive flash cards to reinforce learning. 9 example system exercises teaching you how apply the steps of the Risk Management Framework (RMF). 13 discussions encouraging peer to peer interaction around key topics. 7 end of chapter quizzes with answer explanation to assess comprehension. 142 question post course assessment with answer	ISSOs, ISSMs and other infosec / information assurance practitioners who are focused on security assessment and authorization (traditional C&A) and continuous monitoring issues. Executives who must "sign off" on Authority to Operate (ATO). Inspector Generals (IGs) and auditors who perform independent reviews. Program managers who develop	Classroom based 40 hours classroom based. CPD required, after CICEC. Professionals (government roles) Military, police, civil service etc.

	explanation highlighting areas for further study.	or maintain IT systems. IT professionals interested in improving cybersecurity and learning more about the importance of lifecycle cyber security risk management.	
CSSLP	Instruction from an ((ISC)² Authorized Instructor. Official (ISC)² Student Training Guide. Chapter quizzes. Interactive flash cards to reinforce learning. 17 applied scenarios with corresponding activities teaching you how to apply security through the SDLC process. 24 discussions encouraging peer to peer interaction around key topics. 7 content specific activities, including 6 case studies. 8 end of chapter quizzes with answer explanation to assess comprehension. 160 question post course assessment with answer explanation highlighting areas for further study.	Software developers. Engineers and architects. Product managers. Project managers. Software QA. QA testers. Business analysts. Professionals who manage these stakeholders.	Classroom based 40 hours classroom based. CPD required. Experienced Health Care professionals (2yrs)
HCISPP	Instruction from an (ISC)² Authorized Instructor. Official (ISC)² Student Training Guide. Chapter quizzes. Interactive flash cards to reinforce learning. Real world learning activities and scenarios. 149 post course assessment questions to gauge exam readiness	Compliance Officer. Information Security Manager. Privacy Officer. Compliance Auditor. Risk Analyst. Medical Records Supervisor. Information Technology Manager. Privacy and Security Consultant. Health Information Manager. Practice Manager.	Classroom based 40 hours classroom based. CDP required. Experienced health care professionals (2yrs).
SSCP	Instruction from an (ISC)² Authorized Instructor. Official (ISC)² Student Training Guide. Interactive flash cards to reinforce learning. 20 content-specific learning activities and 12 applied scenarios. 61 content specific activities, including 6 case studies. 8 end of chapter quizzes with answer explanation to assess comprehension. 180 question post course assessment with answer explanation highlighting areas for further study.	Network Security Engineer. Systems/Network Administrator. Security Analyst. Systems Engineer. Security Consultant / Specialist. Security Administrator. Systems / Network Analyst. Database Administrator.	Classroom based 40 hours classroom based. CDP required, after CICEC. Experienced health care professionals (1yr).

3. b Training Facilitation National

It is clear that a novel approach will be required to find time in a busy Curriculum for the adoption of cyber skills training in Schools. Currently Council for the Curriculum, Examinations and Assessment (CCEA) have no guidelines or method to allow new courses to be submitted to their Board. However, CyberSpark Group have been in discussion with the Department for Education in Northern Ireland and they are very supportive of the Project.

We would tailor the courses to the Curriculum to ensure they are scalable to knowledge and ability, given that the students obviously have no commercial experience or experience of the job market, we seek to create that in novel ways to ensure the transfer of skills.

CyberSpark have also been appointed onto the Committee Steering Group for Advanced Manufacturing and Training Centre of Excellence (AMTCE) which works with leaders in education across the Republic of Ireland to enable them to deliver their cyber resilience planning.

CyberSpark is also engaged with Cyberquest to help them deliver their online courses which they are struggling to deliver the skills required. There is a clear need for face-to-face classroom-based learning in order to deliver the results that are required in this rapidly evolving environment. Online learning is struggling to train individuals and this is one of the main justifications for the CyberSpark Academy which will deliver training onsite, as well as in Schools and in the workplace.

See these links to related sites:

https://www.cyberquest.ie

https://www.lmetb.ie/further-education-training/employee-skills-development/advanced-manufacturing-training-centre-of-excellence-amtce/

In addition to delivering programmes in schools, CyberSpark has identified potential trainees amongst groups such as military and police veterans who have learnt many of the innate security skills from their previous service. Such individuals could be upskilled quite quickly through bespoke Cyber Security and IT Training and be reintroduced into the work force as disciplined, trained and security cleared staff. See:

https://www.rutherfordsearch.com/blog/2022/04/cybercrime-costs-to-reach-heights-of-1-pounds-trillion-in-2022

3. c Cyber Security Awareness Training

CyberSpark are well placed to deliver a pilot scheme with local Borough Councils, commercial businesses, and Schools so that participants would receive an initial Cyber Certificate. The training would consist of an Awareness Package, advice on the protection of Networks and how to recognise and thwart Cyber-attacks. This two-day Cyber Certificate Course (CICEC) has been developed by CyberSpark and its partners to equip and qualify individuals and to raise the profile of Cyber Resilience.

By training young adults in cyber skills and providing them with cyber qualifications CyberSpark hopes to develop Northern Ireland into a national centre for skilled, young IT professionals. Companies will be able to benefit from apprenticeships with the Academy and avoid paying the punitive apprenticeship levy.

The Academy will also enable CSIT to cast its net wider in order to populate its Undergraduate and Postgraduate Courses with motivated and qualified young adults. The Academy would be able to deliver skills all year round and not be tied to Academic Terms. The Academy would work with CSIT and Belfast Metropolitan College to deliver training, work placements and Continuous Professional Development. Whilst Queen's University would continue to deliver the highest Academic Qualifications, those delivering cyber security in the commercial or government sectors would skill be able to gain qualifications through the Academy.

In short, CyberSpark would work to:

1. Create a pool of talented youngsters by delivering training in schools and at the Academy.
2. Meet the requirement for skilled coders and programmers in the commercial, governmental, and academic environments.

CyberSpark believes that in future Organisations will have to demonstrate that they take Cyber Security training as seriously as they now take Health and Safety and Equality and Diversity training. They will have to show that they reduced risk to peoples' Data as much as possible by having all staff attain a Cyber Certificate. Tough regulations under GDPR means that organisations can be fined heavily, and this can have a significant impact upon reputation and public confidence. The upskilling of staff and ensuring that they have a Cyber Certificate can be a force multiplier for Cyber Resilience in the workplace nationwide.

4. How It Works

4. a The Project

The CyberSpark Strategy combines a robust Training Programme of classroom-based learning coupled with mentoring is essential to initiate this process. Once established, there will be scope for hybrid training with remote learning and online instruction. The Courses would contribute to each individual's NFQ/UCAS/UKAS points for accredited learning. Potential target groups have already been described namely:

Curricular learning for those in mainstream education

There is an unprecedented skill shortage in the cyber and IT workforce, and this is estimated to be some 2,000,000 vacancies across the United Kingdom (see Appendix A), a surge of approximately 1,000,000 in the last three years. This failure to equip young people for suitable employment means that the Project provides a very real opportunity for young people to embark upon a very lucrative career in Cyber and IT. CyberSpark Academy will offer instructional support at all levels of the Educational System in Northern Ireland. With so many other demands being made of teachers (especially post COVID) they neither have the time nor skills to teach foundational Cyber and IT skills to their children. Further, the Curriculum does not have the resources to introduce commercially available Cyber Courses. CyberSpark plans to deliver

current skills by continually updating its Courses to cope with trends in cyber threats. The Cyber Academy has the freedom to constantly update the learning in its Training packages which will be taught over the seven-year span of secondary education.

Apprenticeships and foundational skills for those out of mainstream education

Live time Apprenticeships offer the flexibility to deliver training in line with the market needs and current threats. The United Kingdom has a worrying number of cyber jobs which cannot be filled with no relief in sight. This has resulted in a slowdown in foreign and national investment from the Tech companies which are amongst the most dynamic and fastest growing sector of the Economy. The Courses being offered by the Academy will help to generate staff to fill these vacancies. These Courses can be replicated across the UK and Ireland whilst offering Apprenticeships and Certification for staff should prove an attractive prospect to forward-thinking Organisations. Commercial Companies can obtain Government funding for the training of Apprentices and can thereby reduce their exposure to the Apprenticeship Levy Funding would be available for training the following:

School leavers

Mid-career changers

Mothers returning to work

Jobseekers and unemployed

Veterans

Youth Justice Groups

Training such Groups will provide a clear route to employment, offer progressive transfer of skills and establish a firm base in the Cyber and IT Community across the UK and Ireland thus providing for the prospect of secure and well-paid career. The physical location of the Cyber Academy will allow for a concentration of Commercial Companies, Government Agencies and Academic Institutions thereby creating a Cyber Hub – a unique ecosystem which will combine education, research, job placements and full-time employment opportunities all on the one site.

4. b Outcomes

The non-existence of an effective “Resilient by Creation” professional support system for both School leavers and those looking to change career in Northern Ireland will be addressed through the full implementation of the “Resilient by Creation Programme”. The establishment of this Programme will address completely those who are leaving and those who have left full time education. The Academy anticipates approximately 1,000+ participants in the first year with the following outcomes:

- Participants will have suitable Mentors (for mutual assessment of appropriate development and future employment opportunities).
- Participants will be supported in acquiring skills appropriate for commercial employment.
- Between 60-70% of Participants will move into employment or further education development.
- 80-90% of Participants remain in employment for the duration of the Programme and beyond.
- Employment re-integration of 100% of Participants.
- Employers in the Community gain a skilled workforce, with a mentoring arrangement established between the Participant, the Employer, and the Academy.

The outcomes will be measured through:

- Training and development records.
- Tiered Mentoring system.
- Personal interviews.
- Employment records.

- Employer interviews.
- Appraisals.
- Educational Development.

The Programme will be evaluated using qualitative and quantitative methods, providing feed back into the learning cycle thereby leading to continuous improvement of the Programme, increased benefits for the Participants and the ability to the assess value for money of funding.

The Programme with its “Resilient by Creation” approach using the mentoring system has holistic qualities; the mentoring helps to break down barriers and obstacles that often get in the way of those who are leaving or have left full time education, looking to re-enter the employment sector, or are changing career. The close relationship developed by the Mentor / Mentee system in the Apprenticeships will bring in to play the confidential friendship and guidance required by the Individual. The Mentors will be like minded individuals who understand the strains and stresses of embarking upon a new career. The ability for the Mentees Apprentices to have a platform to off load their fears and concerns in a confidential environment will enable the Academy to identify any help and guidance that might be required. CyberSpark will construct a clear path to employment. Following the global pandemic there remain significant barriers to success such as:

- Depression.
- Housing difficulties.
- Financial advice.
- Health and well-being issues.

4. c Leadership, People and Resources

The Programme was developed by a former service person who served over 24 years in the Services and is an experienced Mentor. The Group has sourced a number of experienced individuals who sit on its central Board. These individuals have significant experience in commerce, industry, and government with ready access to a network of experts and influencers who will support the Academy. The project also has the support of a number of reputable Cyber and IT Companies who have embraced the Academy concept and recognised how it will help to support and develop the local, regional and national economy. The Academy has partnered with (ISC)², a globally recognised Company with a strong network of cyber security training experts which will be responsible for the face-to-face training.

4. d Financial Support

The Cyber Academy Board includes Accountants, Lawyers and other suitably qualified Experts who have governance powers and oversights to ensure funds within the Programme are used to best effect. The Project will exist as an Education, Retraining and Recruitment Programme utilising a range of private and public funding to develop and deliver the Programme. Over time the profits generated by the the Academy and its Campus will be reinvested in the Programme. The Not-for-Profit role of the Academy is perceived as being central to its success.

There are a number of local and international Companies who have expressed interest in employing Graduates of the Academy. Training at the Academy with a recognised Cyber Certified Qualification for each Graduate should overcome the reluctance of employers to take on those coming straight out of education, other careers or those who have either been unemployed or engaged with the Criminal Justice System.

It is anticipated that Government funding will only be required during the start-up phase after which the Academy will be supported by industry based on the campus and the delivery of Cyber Courses by training for Schools, Government Organisations and Commercial Enterprises.

4. e Ambition

The Academy has the potential to become a very attractive option for School leavers who wish to embark on Apprenticeship training or avoid an expensive and lengthy journey through University. Courses at the Academy should prove popular with both local and international students. A strong relationship with industry and public bodies will provide opportunities for work placement and permanent employment for students from the Academy.

4. f Leverage

CyberSpark Group has established a robust network in Northern Ireland with Education, Commerce and Industry supported by the wider political structures. Each recognise the potential benefits that would flow from the successful delivery of the Training packages offered by the Academy. There is strong political support from the Executive Office of the Northern Ireland Assembly who are keen to deliver upon the promises of cyber employment made in the New Decade New Approach Deal which promised to *"Promote Northern Ireland as a global cyber security hub, building on its blend of world-class talent, leading forensic science expertise and tech research excellence to achieve 5,000 cyber security professionals in Northern Ireland by 2030."*

4. g Sustainable

CyberSpark accepts long term sustainability cannot nor should not be dependent upon continuous Grant Funding which is why social and economic structures are in place to help sustain the Programme in the future with the negotiations well underway for the signing of Contracts for the programme.

The intention is that the Academy will eventually deliver a completely self-sustaining Programme. The First Year of the Programme is crucial for the establishment of working relationships with Industry and Government Agencies. No other Programmes exist that offer the "Resilient by Creation" approach and the "whole of Ireland" nature of the Academy means that strong cross border connections will allow young people from both Jurisdictions to benefit through the Academy's Cyber Training Programmes.

4. h Needs

Northern Ireland enjoys a unique position in the United Kingdom as it has retained an advantageous relationship with the European Union. The land border with the Republic of Ireland enables a close relationship to develop between the two Jurisdictions and for Northern Ireland to benefit from of the US inward investment in high tech Industries across Ireland. Working closely with colleagues in Ireland there is an opportunity to provide cyber training for young people thereby providing them with a very real prospect of permanent employment upon completion of Courses at the Academy. This will help to build political and social confidence and boost both economies.

There are two sets of needs which will be met through this Programme. Firstly, the need of Individuals to become skilled and qualified in cyber in order to achieve permanent employment. This is matched by the ongoing needs of Organisations to have Individuals who are trained and competent to protect their Networks and information stored therein. The Academy has the potential to meet both sets of needs by providing agile, appropriate, and affordable courses. The demand for those with strong cyber skills will only increase especially in light of the investment being made in individuals State sponsored operatives and cyber criminals in offensive techniques which far outstrips the current investment in defensive measures.

CyberSpark has been appointed as a main advisory group to the North / South commitment on skills and training in cyber. The company is represented on the main steering group through the AMTCE in Dundalk which reports directly to the cyber directorate of the Irish Government. Through the Resilience Task Committee role, CyberSpark have been instrumental in creating a **Cyber Corridor** to develop the skills necessary for Cyber and IT employment throughout Ireland.

4. i Community Education Programme

Northern Ireland society still carries scars from the Troubles and remains a post conflict environment with its own set of challenges and potential problems. This is recognised by the CyberSpark Group which is committed to playing its part in creating training and employment opportunities for young people, no matter their background. There is a firm belief that a strong economy, where reward is shared fairly across the whole community, will lead to a peaceful and successful economy.

In a Country where schooling still remains largely segregated, the Academy will bring together young people with a shared passion for IT and present them with a chance of excellent training and employment opportunities. By reaching into mainstream education and exposing young people to Coding and Cyber Security it is anticipated that a path will be established for those who display aptitude by providing them with the skills required to attain both Professional and Academic Qualifications. Northern Ireland has seen upsurge of investment by Cyber Companies, Banks, Legal and Accountancy Firms, Consultancy, HR and Technical Companies. This "Nearshoring" is due to the high academic achievements of schoolchildren most of whom, despite the fact that wages are lower in Northern Ireland than in London or Dublin, seek to stay in Northern Ireland long term with the same employer. This is not a new phenomenon and shows

that success breeds success. The following release was published in TECHWATCH 2017:

“So the explosion in cyber security companies flocking to Belfast - leading to the city being dubbed the ‘cyber security capital of Europe’ - has largely gone unnoticed by the press and the broader tech community.

Rapid7, a provider of software-based security solutions, is one of a number of companies that have established a presence in Belfast over the last two years. Relocated employees have been learning about black taxis, murals and the importance of carrying loose change because not all shops accept card payments. Its staff blogs are littered with posts like this one, from transplanted US employee Matt Hathaway: “After expressing interest in a townhouse recently occupied by university students, I had to impatiently wait 24 hours for my US bank to transfer the housing deposit. If you ever find yourself living in another country, please tell me if you find a process to transfer foreign currency without feeling like a criminal.”

After acquiring local startup MailDistiller, California’s Proofpoint - a provider of cloud-based security tools - announced in August that it was opening an office in the city, with a plan to create 94 jobs. Alert Logic, another Security-as-a -Service provider, also launched a local base. Now, Belfast has the highest concentration of cyber security jobs in Europe, even more than London, says David Crozier, CSIT’s Technical Marketing Manager. ”We had Jeremiah Grossman and his WhiteHat Security team here on their first inward investment visit 20 months ago. Their announcement [about their move to Belfast] was only made last December. Cyber security companies are coming here for a number of reasons including the Invest NI support package and the research and skilled graduates flowing from CSIT. It’s an attractive proposition.”

So what’s attracting them? Aside from the financial incentives offered by Invest NI to sweeten the deal, Hathaway says a tough recruitment market in the States is forcing companies to look abroad for talent. “I think a lot of it was the culture and the opportunity for hiring because it's become very, very challenging to find innovative developers in the US because of the number of companies we're competing with on a day to day basis. Not many cities - or, if you want to compare it to states, I guess - have put in the effort that Northern Ireland has in fostering software development. I mean, the universities here all have intense programmes, they have year-long placement programmes which we're using heavily - we have nine placements now, we'll have 18 later in the year - and it's just there's so much emphasis on that. Software is what this city wants to be known for.”

The presence of CSIT is also helping lure Companies to Northern Ireland. As well as being an Academic Centre of Excellence in Cyber Security Research (a scheme accredited by GCHQ, amongst others), CSIT offers an MSc in Cyber Security and PhD programmes, providing - as Crozier pointed out - a steady flow of trained talent. Rapid7, Hathaway says, has regularly conversations with CSIT about potential collaborations.

For Stuart Laidlaw, CEO of London-based startup, Cyberlytic, creators of threat analysis tool Cyber Threat Profiler and an Amadeus Capital Portfolio Company, it was CSIT and the talent supply from Queens that persuaded them to establish their R&D team in Belfast. *“We're based in London but we're also based here. So all our research and development team as we grow will be based in Belfast and we'll co-locate here, hopefully with CSIT, that's the idea, that's the plan. It wasn't an easy decision for us to make because we are London [based] as well but just access to the talent and the brains here."*

The rapidly forming cluster of Cyber Security Companies in and around Belfast should also have benefits for the wider startup scene, if properly supported. For years, there has been debate about how to get big name VC’s to take an interest in NI, in the same way they do Israel or Berlin. With VCs like Van Someren now making visits, it looks like Belfast’s prospects are starting to improve.

CyberSpark Group recognised that the demand for cyber skills remains high but that the pool of IT professionals is rather shallow. Unless more skilled personnel become available the attraction of Northern Ireland as a place to base a Cyber Company will begin to fade.

If a route from Schools to the Academy can be established and then into employment then there is a real chance that Northern Ireland can live up to its potential as a Cyber Hub and provide world beating services to Companies, local, national and international, based in the Province and further afield. With CyberSpark sitting on influential Committees both North and South of the Border it is believed that there is real potential to influence the future of the economic and educational environment of the whole of Ireland.

5. Long Term Strategy / Expansion Plans / Sourcing Customers

5. a Assistance

It is clear the current demands upon the Teaching Profession mean that there is no spare capacity to deliver Cyber Training in schools without external assistance. Whilst most Schools have sufficient laptops and IT suites, they are now used far less than when first established. Perhaps the assumption is that as children have mastered their Smart Phone, there is little that they need to be taught about IT. In the same way that Schools have brought in external providers to deliver sports training and physical education, a similar template is required if Cyber Training is to be introduced to the Curriculum. Whilst most of us last encountered algebra whilst at School, exposure to cyber threats and scammers remains a daily occurrence for most people. Preparing children for such challenges should be a core subject. It is envisaged that Teachers would support the delivery of cyber lessons in Schools by accompanying their class to assist in coordination and discipline.

The current programme is planned as follows

1. Pilot 1 is being run for Key Stage 2 Pupils (Primary Year 7) this will take the form of an introduction to coding through a Micro:bit Coding Course.

2. Pilot 2 is being run for 47 Groups within the Community Projects in Northern Ireland including Youth Justice Groups.

3. Pilot 3 is being run for Veterans' Groups and mid-career changers.

4. Pilot 5 is being run for Cadet Force Groups.

These Courses will be in the format of a standardised 2 day Cyber Certification Course which will provide valuable information to assist the planned continuous development of such Courses. Initially these Courses will be funded by private funding and Government Assistance Funds, notably the National Cyber Resilience Fund which has £22,000,000,000 available for suitable Projects.

5. b Credibility

CyberSpark has had ongoing discussions at Ministerial level and the Executive Office is in support of the project. CyberSpark has also been appointed to the Cyber Directorate Advisory Committee of the Republic of Ireland to assist in steering the cyber resilience planning for the entire Island of Ireland. This gives CyberSpark the opportunity to guide the standard cyber resilience plan using the Academy's Cyber Courses which have been devised and accredited by Global cyber experts. The pilots will be attended by the Minister for Education and the Minister for Communities, as well as Representatives from CCEA. These Pilots will demonstrate the need for such Courses and the ability of the Academy to devise and implement them. The Minister for Education has already been supporting CCEA attendance. See:

https://ccea.org.uk

5. c Expansion Plans

The Academy proposes to start with 100+ individuals per month in the Cyber Certificate Courses in the first year by training them in Cyber Security awareness and educating them with Cyber Skills suitable for industry courses. The individuals will be assessed and those who show greatest aptitude will be offered Apprenticeships, with a view to eventual employment with the Security Operational Centre (SOC) facilities for Cyber Security.

The Academy would also seek to train / upskill current workforces within existing Academies and in industry to operate secure networks within Government Departments and Private Industry, including the Financial and Supply Industries.

The Academy would retain suitably qualified individuals who received their training at the Academy for the purpose of hiring them out to Companies to carry out security audits. Currently there are 2,000,000 unfilled cyber vacancies in the UK alone and CyberSpark believes that it can attract in the region of 20,000 jobs over a 5 – 8 year period. Contracts will be entered into with smaller sized Companies to conduct day to day cyber security for their Servers.

5. d Resource

The Academy will conduct its own internal training using the resources within its established Networks until such times as sufficient Staff have received the necessary education in Cyber Awareness and advanced Cyber Security Audits. Thereafter these Staff Members will train individuals attending the Courses at the Academy's Training Centre leading to globally recognised Teaching Certificates By such ongoing training the Academy expects to be at the centre of any strategy to strengthen the National Cyber Resilience Plan through its ability to help train individuals to clear the back log of training required in current Government Departments, the Services and Industry.

6. Economic Value

The current number of cyber IT professionals in Northern Ireland stands at some 2,600 – currently below the requirement for the regional economy and below market share for the UK. "*The estimated total revenue of the cyber security sector in the United Kingdom in 2021 was £10.15 billion. This was the largest revenue within the period highlighted, representing a value almost twice as high as the one recorded in 2017. While this indicated a positive forecast, the 2020 estimate was made prior to the coronavirus pandemic."* (Justina Alexandra Sava Oct 19, 2022)

The Republic of Ireland has just under 7,500 cyber operators and their presence generates an annual GVA of €2.1 billion (approx. £1.8 billion) for the national economy. CyberSpark's approach could match this figure within 5 to 8 years. With the support of government in Stormont the aim is to create a vibrant cyber cluster in Belfast and support a cyber corridor across the border into Ireland. See:

https://www.cyberskills.ie/media/cyber-skills/site-assets/pdfs/Cyber-Ireland-Report-V8-(pages).pdf

7. The Proposal

CyberSpark will introduce cyber training into the School Curriculum in the following manner:

- Primary (KS2) year 7, will commence in April 2023 focus upon Primary Schools in the Louth/Meath and Area delivering the 3 modular 1 hour lessons to all students in KS2. This is a measured approach as it does not interupt the KS2 students who are waiting to progress to Secondary School. The courses will prepare them for KS3.

- Secondary (KS3) years 8 -10, will commence September 2023 where the students will gain the foundational knowledge as part of the curriculum which will be 6, 1 hour lessons each term. There will be online assistance available to students.

- Secondary (KS4) years 11-12, will commence September 2023, the students will be prepared to upskill in commercial grade programming, coding and design. This will be entry level skills and the students will gain a commercially relevant qualifacation through the Academy, this can be aligned with leaving Cert and higher level leaving cert (in line with NFQ)grades.

- Secondary (KS5) the contiinual development of the student will take place and will commence September 2023, giving the student the higher grade of the commercial qualifacation, at that point the student will be ready for employment, or moving onto more specialised disciplines taught in University (AIT,MTU,UCD,CSIT,ESIT, Belfast Met ETC).

- Adult learning would commence in February 2023 depending upon direction from the Department for the Economy. The programme would upskill and qualify adults in courses which would lead to employment in the IT industry in Northern Irerland. The courses have global accreditation.

The cost of the initial roll out and the programmes would be embedded into education and higher national learning in the review and research stage would cost between up to £3million; the implimentation throughout Ireland would be considerably more.

To put this in context, CyberSpark seek to train 800 people in cyber security in the 18 months of the research; the GVA on those 800 individuals could return some £180 million euro to the economy. The current jobs gap in the UK sits at over 100,000 cyber professional so by concentrating on this discipline

we should be able to attract 10% of that number to Ireland, growing our cyber professional output to around 18,000 in 8 years.

Primary KS2	Course Name	Delivery Mode	Duration
Year 7 Key Stage 2 (KS2)	**MICRODOT programming**	**Face-face learning Module exercises**	**3 days 2 hr duration**
Course Overview	1. A (very) brief history of computers, the invention of the transistor, invention of the CPU through to the future; 8 bit computing through to 64bit computing, the future… qubits (quantum computing). 2. Introduction to micro-controllers (PIC, Atmel, Arduino and Micro:Bit). 3. Introduction to programming languages and development environments (Basic, Scratch, Python, Java, C++ / C#). 4. Physical introduction to the Micro:Bit hardware (Assembling of the Micro:Bit kit; enclosure, battery box and USB cable). 5. Introduction to the Micro:Bit programming environment (scratch - the simplest environment to get started). 6. Supported learning, hand-on with the children programming boards and experimenting		
Learner Profile	All students participate		
Secondary KS 3-4	**Foundational IT**	**Face-face learning Module exercises**	**All terms 6 x 1hr lessons per term KS3 10 x 1 hr lesson per term KS4**
Course Overview	The aim of the lessons in Key stage 3 (KS3) is to provide students with the foundational knowledge to operate proficiently in the coding and design framework. The foundational knowledge required is of a higher standard than currently taught in curricular education. Prework, workshops including delivery of cyber content & student feedback. Potentially the student will gain valuable knowledge for future careers, even if they do not choose cyber security. The aim of Key stage 4 (KS4) is to provide the students with the knowledge and skills required to move directly into commercially relevant qualifacation at (GCSE&A level),on leaving education at 16-18, the students have the ability to progress immediately at entry level coding and cyber skills. The ease of process to degree, masters and PHD is already there but will become more readily accessable. The students with all of these techniques will have the ability to deliver professionally taught commercial skills. This is a new approach which declutters the route to employment, Private firms and government departments will immediately feel the benefits of the students abilities.		
Learner Profile	All students participate in KS3, Students can then select course at KS4		