A V-LINC Analysis of Northern Ireland's Cyber Security Ecosystem.

Dr John Hobbs, Dr Eoin Byrne, Dr Cliodhna Sargent and Tabona Kuli

V-LINC Research Group, Cork Institute of Technology, Ireland.

E-mail: john.hobbs@cit.ie ;

Published Date: 01-09-2020

Abstract

According to fDi Markets Intelligence (2020) Northern Ireland is recognised as the number 1 international investment location for US cyber security development projects. The region is now home to a number of international companies, world renowned university research and innovative start-ups delivering global cyber security solutions. The cyber security sector employs almost 1,700 people and is on course to generate over £70 million in salaries each year, with over 75 companies operating in Northern Ireland (Computer Weekly, 2019). There is an ambitious target of having 5,000 employees in the sector by 2030 (NDNA, 2020). Companies in Northern Ireland have built upon expertise in developing cyber security products and services in Northern Ireland are in the areas of: Cyber Professional Services, Threat Intelligence, Monitoring, Detection and Analysis, Endpoint Security. Whilst expertise in emerging sub-sectors such as IoT Security, SCADA and ICS, Post-Quantum Cryptography is developing rapidly (DDCMS, 2020).

V-LINC, a methodology which identifies, records and analyses the linkages that firms in clusters engage in, is applied to the NI Cyber Cluster in Northern Ireland. V-LINC was developed in Cork Institute of Technology to enrich academic literature on clusters. It provides visual information on the geographic footprint of cluster ecosystems and measures the business impact of cluster linkages. Through an understanding of the various linkages that firms in a cluster engage, targeted policy recommendations can be made to build on strengths and aid weaknesses.

As the Northern Ireland cyber security sector develops and expands it is important that industry players, business support organisations and policy makers understand how the ecosystem operates both within Northern Ireland as well as its external relationships forged beyond the region, so that collaboratively, they can deliver growth and employment through supportive policy.

Keywords: *V-LINC, industry cluster, ecosystem, cyber security, mapping.*

CIT CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

InterTradeIreland

NI CYBER
Northern Ireland Cyber Security Cluster

This report was funded by InterTrade Ireland.

Introduction

This paper represents a collaboration between the Cork Institute of Technology and NI Cyber who partnered to apply V-LINC to the cyber security specialisation in Northern Ireland.

The cyber security industry in Northern Ireland has been growing steadily over the past decade, it presently employs nearly 1,700 people. It is on course to generate more than £70m in salaries each year, according to Máire O'Neill, Professor at Queen's University Belfast speaking at the 9th World Cyber Security Summit. "With the unrelenting pace of digital adoption, the role of cyber security has never been more significant. Its importance to our lives and livelihoods is increasing exponentially and those with the skillsets to contribute to this vital societal need will always have a place in the new economy."

In 2017 Centre for Secure Information Technologies (CSIT), kick started, what would in time become NI Cyber, when they brought together sixteen companies, a mixture of cyber start-ups SMEs and large firms, for a design thinking innovation workshop to see if there were opportunities for collaboration around addressing the skills gap through training in Northern Ireland and connecting the R&D ecosystem. The group connected with the Open Web Application Security Project (OWASP) and Information Systems Audit and Control Association ISACA to collaborate, and more cyber focused firms began to participate. In summer 2019, funding was sought for a Programme Manager through Invest Northern Ireland's – Collaborative Growth Programme – Phase 1. This support is for SME-led networks requiring facilitation support to scope out innovative collaborative projects with the potential to increase business competitiveness.

In late 2019, funding was allocated to NI Cyber and they have started in earnest to develop their network, with the number of participating organisations increasing to 40. The group are now looking to develop a longer-term strategic perspective, as they seek to develop into a European Style Cluster organisation – and are looking at core funding models from a Phase 2 application to Invest Northern Ireland's – Collaborative Growth Programme or perhaps dedicated cluster funding from the Department of Economy, Northern Ireland – or a combination of both. At this stage of NI Cyber's development, participants and policy makers must understand how the ecosystem operates both within Northern Ireland as well as its external relationships forged beyond the region, so that collaboratively, they can deliver growth and employment through supportive policy.

The paper begins with an explanation of V-LINC, a methodology which records, categorizes and measures the business importance of linkages that cluster firms participate in, along with the facility to show linkages on geographic maps of appropriate scale. Linkages (see Figure 1) between firms and other organisations are at the heart of how clusters function. Linkages are defined (Hobbs, 2010; p 221) as "relationships that enable exchange of goods, services, personnel, information, ideas, expertise, grants and other supports to business that occur between two or more parties, over a sustained time period." Next, the paper comments on the scale of the cyber security industry in Northern Ireland, then reviews findings from V-LINC analysis on the linkages of a sample of cyber firms in Northern Ireland. The analysis includes: the distribution of linkages by category, by geographic scope, and by their business impact as recorded by company employees who engage in the linkages. V-LINC maps illustrate the linkages at different geographic scopes. Arising from the analysis a judgement is made about the extent of cluster activity in the cyber security industry in Northern Ireland. The paper closes with recommendations on how to strengthen and support the NI Cyber Cluster in Northern Ireland.

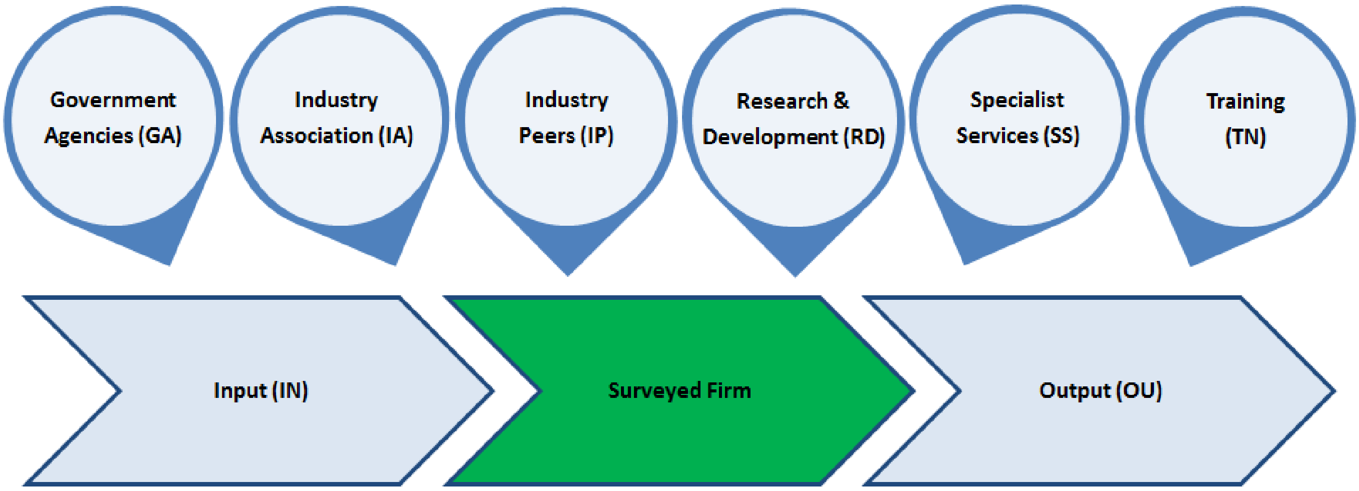


Figure 1: The Eight V-LINC linkage categories analysed for each firm.

The authors would like to acknowledge the contributions of Judith Millar, Centre for Secure Information Technologies (CSIT) at Queens University Belfast; Linda Jamison, Collaborative Networks Manager at Invest Northern Ireland; Dr Krystal Miller, University of Ulster and Scott Carson, NI Clusters Policy Manager, at the Department for the Economy.

V-LINC: Visualisation of Linkages in Networked Clusters

V-LINC[1] is a methodology for identifying, recording and analysing the linkages that firms in clusters engage in. It categorizes these linkages, and groups them by geographic scope. Furthermore, V-LINC records the business impact of linkages based on the perceptions of firm personnel who engage in the linkages with other companies and organisations. Data for V-LINC is collected by structured interviews of company personnel. Likert scale questions are employed to gauge the business impact of individual linkages. V-LINC maps give a visual representation of the relative reliance on Local, National, European or International linkages of a company and when combined, of a cluster (Figure 2). V-LINC facilitates policy development at local, regional and national levels, through the aggregation of data from a sample of firms. Confidentiality of firms' linkages is maintained throughout.

V-LINC assigns company linkages to one of eight categories (Figure 1). Besides linkages along the supply chain, namely those which provide Inputs and Specialist Services to firms, and Output linkages which provide markets for goods produced, V-LINC adds five other categories of linkages: those with Industry Peers, with Industry Associations, with Research & Development partners, with Training partners and with Government Agencies. The linkage categories in V-LINC derive from Porter's (1990, 1998a and 1998b) discourse on the interactions and relationships of companies in a cluster. V-LINC responses collected through structured interviews combine to reveal the business impact of linkages by expert company personnel. Likert scale responses convert qualitative judgments into quantitative data which are subject to further analysis. The importance of the linkages are recorded and scored between 0 and 40, then arranged into four business impact bands based on their importance: High (>30 to 40), Medium (>20 to 30), Low (>10 to 20), or Tenuous (0 to 10).

The result of the V-LINC analysis is information that can inform cluster policy: which linkages exist, if any, between players, and the strengths of the bonds between different actors. Most importantly, at this stage, cluster organisations and policy makers will know all linkages between the private sector, academia, and government, and can subsequently implement policies to target weak points in a cluster, or to develop local skills. Next, the rationale for applying V-LINC to the cyber security sector in Northern Ireland is outlined

[1] V-LINC is a hybrid methodology developed by Byrne (2016). He combines the *'Four i Linkage Scale'* (Hobbs, 2010), network theory and visualisation techniques to map and trace cluster ecosystems. Linkage categories and business impact bands are defined in Byrne (2016).

Cyber Security in Northern Ireland

According to fDi Markets Intelligence (2020) Northern Ireland is recognised as the number 1 international investment location for US cyber security development projects. The region is now home to a number of international companies, world renowned university research and innovative start-ups delivering global cyber security solutions. The cyber security sector employs almost 1,700 people and is on course to generate over £70 million in salaries each year, with over 75 companies operating in Northern Ireland (CyNation, 2019). There is an ambitious target of having 5,000 employees in the sector by 2030 (NDNA, 2020). Companies in Northern Ireland have built upon expertise in developing cyber security products and services in Northern Ireland are in the areas of: Cyber Professional Services, Threat Intelligence, Monitoring, Detection and Analysis, Endpoint Security (including Mobile). Whilst expertise in emerging sub-sectors such as IoT Security, SCADA and ICS, Post-Quantum Cryptography is developing rapidly (DCMS, 2020).

McKee (2019) reports that since 2014, Invest NI has offered £68 million in financial assistance to firms involved in cyber-security. The sector is composed of more than 75 companies, ranging from global firms employing more than 100 in a department to smaller and micro businesses. Queen's University, Ulster University and Belfast Metropolitan College cater for the education needs of the cyber-security professionals in NI, who can earn more than £43,000 on average (DCMS, 2020).

The European observatory for clusters and industrial change (EOCIC) provides policy support to existing or emerging cluster initiatives at national and regional level. A location quotient (LQ) is a way of discovering the industries or occupations that are truly unique and specialized in your regional economy (compared to the national average). The European Observatory for Clusters and Industrial Change Mapping Tool does not showcase cyber security as a sectoral specialisation with digital industries (Figure 2) only scoring a 0.42[2]. What this means is that if digital industries in Northern Ireland accounts for 0.42% of jobs when digital jobs nationally (UK) account for 1%, then the digital industries have an LQ of 0.42, which means that this industry is 0.42x more concentrated in the Northern Ireland than the national regional average. Figure 2 showcases the fact that bio-manufacturing is the only sector in Northern Ireland which is identified as a specialisation with a Location Quotient of 1.62 when compared to the national average.

[2] It must be highlighted that the European industrial activity classification (NACE) system, has difficulties as due to its nature it does not align with new technological sectors such as cyber security. Hence some elements of cyber security may be captured in digital industries and others may be aligned with other segments e.g. electrical equipment, telecommunications and computer programming, consultancy and related activities.

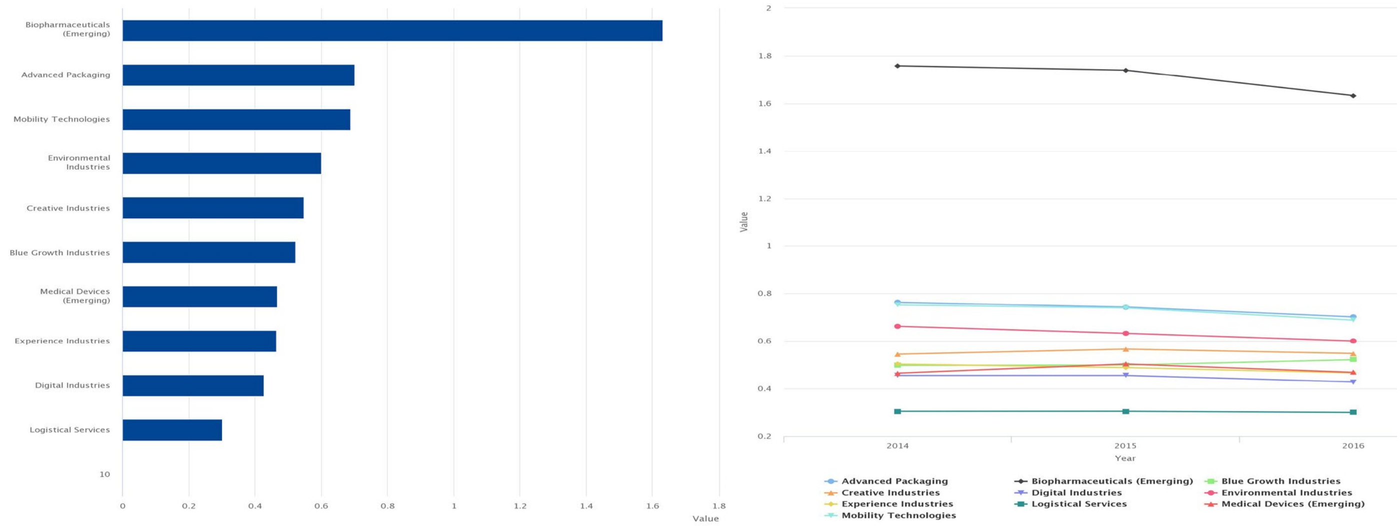


Figure 2: UK – Northern Ireland Profile by Sector for Specialisation & Sectoral Evolution.

While the NI Cyber Cluster in Northern Ireland has not been identified as a cluster by the European Clusters Observatory, or for economic policy development, it is an important sector not solely for its growth, but as it is a cross-cutting industry which affects growth and innovation in other sectors in Northern Ireland and across the UK. Investigating the linkages that Northern Ireland firms in the cyber security cluster engage in can prove beneficial in understanding the cluster and developing policy recommendations for future growth.

One critical support element within Northern Ireland which has been critical to the development of the sector is the Centre for Secure Information Technologies (CSIT), Queen's University Belfast, which is the UK's Innovation and Knowledge Centre. As part of its mission to work with industry, CSIT provides academic and engineering support for the London Office for Rapid Cybersecurity Advancement (LORCA), aimed at helping start-ups to scale their organisations at pace, to access and grow into new markets, secure further investment, and recruit and retain the best talent. The sector is further boosted by the expertise in Ulster University (UU) which conducts world-leading research in intelligent systems, assistive technologies, next generation networks, and semantic analytics, within their four highly active research groups and centres. These include: Artificial Intelligence; Cognitive Analytics Research Lab (CARL); Intelligent Systems and Pervasive Computing research groups and centres.

Another element in the cyber security ecosystem is the Digital Catapult Centre Northern Ireland, in the Titanic Quarter. Digital Catapult focuses on being at the forefront of innovation by building partnerships and bridging the gap between industry and academia, whilst working closely with Invest NI and the Department for the Economy. The centre is focused on helping large and small organisations work smarter and more efficiently by realising and adopting innovative digital technologies. Working closely with a network of organisations from all over the region, the Digital Catapult supports companies based in the region to scale and grow. It forms a gateway for companies to access a range of digital services.

The use of digital technology has a growing influence in a range of sectors including manufacturing and the creative industries. Through the delivery of an innovate programme of events the Digital Catapult seeks to accelerate early adoption of emerging technologies and exploit both the commercial and research opportunities they can offer. The Immersive Lab, based in Belfast, is available to all organisations and businesses, large and small, to experience the latest immersive technologies as well as demonstrate and test their content.

Digital technology is at the heart of the UK economy, underpinning growth through both the development of new technologies and the provision of services to businesses and consumers. It is through support and partnership with researchers and Universities that Digital Catapult Northern Ireland will ensure Northern Ireland can meet the growing skills demands of the digital sector and its future workforce pertaining to artificial intelligence and immersive content.

Digital Catapult Northern Ireland signed a MOU with BBC NI to create opportunities to reach new audiences, utilise emerging novel technologies, and use content from the BBC Rewind archive portal. The relationship will see BBC Northern Ireland and Digital Catapult work together to share facilities, workspaces, equipment, and expertise, advance projects within the immersive sector, develop talent and skills within both organisations, and work together on exhibitions, workshops and events (Digital Catapult, 2019).

This research has been funded by InterTradeIreland, as part of their work to connect sectors on the Island of Ireland. The support of Judith Millar, Business Development Manager, Centre for Secure Information Technologies (CSIT) at Queens University Belfast; Linda Jamison, Collaborative Networks Manager at Invest Northern Ireland; and Scott Carson, NI Clusters Policy Manager, at the Department for the Economy has been invaluable in organizing interviews and connecting with the sector in Northern Ireland. V-LINC has been applied to a sample of 10 cyber security firms based in Northern Ireland (predominantly in Belfast). Fourteen face to face meetings were held with personnel from these companies to gather information regards to their key relationships. These meetings uncovered 251 firm linkages (Table 1). The term Respondent Firm Group (RFG) relates to the summation of data for the ten cyber security respondent firms.

V-LINC Analysis Results: Cyber Security Northern Ireland.

Table 1 and Figure 3 showcase the firms in Northern Ireland who participated in Mapping the Cyber Island V-LINC analysis and the respective size of their operations. It provides the percentage of linkages they report in each of the eight linkage categories, along with the total number of linkages they engage in. It also distinguishes the total numbers of linkages per category for the cluster. Table 1 reports that the most frequent linkages are in Outputs, which account for 40% of linkages reported; followed by Training (12%) and Inputs (10%). This is not unexpected, as firms exist due to the continued development of revenues and customers. Inputs and Training also feed into a firm's product and service offering. The least frequent linkage categories are Industry Peers and Research both accounting for 6% of all linkages, respectively. This may indicate difficulties in forming collaborations both from a business and research perspective.

Company Name	Firm Size	GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Allstate	**Large (250+)**	12%	3%	9%	15%	24%	15%	3%	18%	**33**
Ampliphae	**Small (<50)**	11%	7%	11%	0%	54%	4%	7%	7%	**28**
AnsecIA	**Small (<50)**	4%	26%	0%	0%	39%	0%	9%	22%	**23**
B-Secur	**Small (<50)**	5%	10%	26%	8%	26%	10%	13%	3%	**39**
Cygilant	**Small (<50)**	6%	6%	12%	12%	35%	6%	18%	6%	**17**
Cynash	**Micro (<10)**	17%	8%	0%	0%	33%	8%	17%	17%	**12**
Kainos	**Large (250+)**	12%	6%	3%	12%	45%	6%	9%	6%	**33**
Liberty IT	**Large (250+)**	6%	6%	17%	0%	50%	0%	11%	11%	**18**
Skurio	**Small (<50)**	12%	8%	8%	0%	42%	4%	8%	19%	**26**
Vertical Structure	**Micro (<10)**	5%	9%	9%	0%	59%	0%	5%	14%	**22**
RFG Average		**9%**	**9%**	**9%**	**5%**	**41%**	**5%**	**10%**	**12%**	**25**
Total (n)		**22**	**22**	**26**	**14**	**100**	**15**	**23**	**29**	**251**
Most Populous (Rank 1-8)		**6th**	**6th**	**3rd**	**8th**	**1st**	**7th**	**4th**	**2nd**	

Table 1: Distribution of Linkages by Category and by Firm[3]

Geographic proximity of firms, local connections with other firms or organisations, and face-to-face interaction, play a central role in cluster theory and are attributed to producing higher growth and innovation in clusters. Porter (1998a, p 226) believes, "a cluster is a form of network that occurs within a geographical location, in which the proximity of firms and institutions ensures certain forms of commonality and increases the frequency and impact of interactions."

[3] Note to Table 1: The eight linkage categories are: Government Agencies (GA); Industry Association (IA); Industry Peers (IP); Inputs (IN); Output (OU); Research & Development (RD) Specialist Service (SS) and Training (TN) linkages.

However, modern advances in communication and technology have impacted the need for geographic proximity and allow connected firms to be more widely dispersed across a region, or even countries. Firms may source Inputs from multiple regions, may engage in R&D with research organisations in foreign countries, and sell into international markets. Therefore, it is important to look at the geographic scope of linkage categories, and also the business impact of linkages which occur over different geographic scopes.

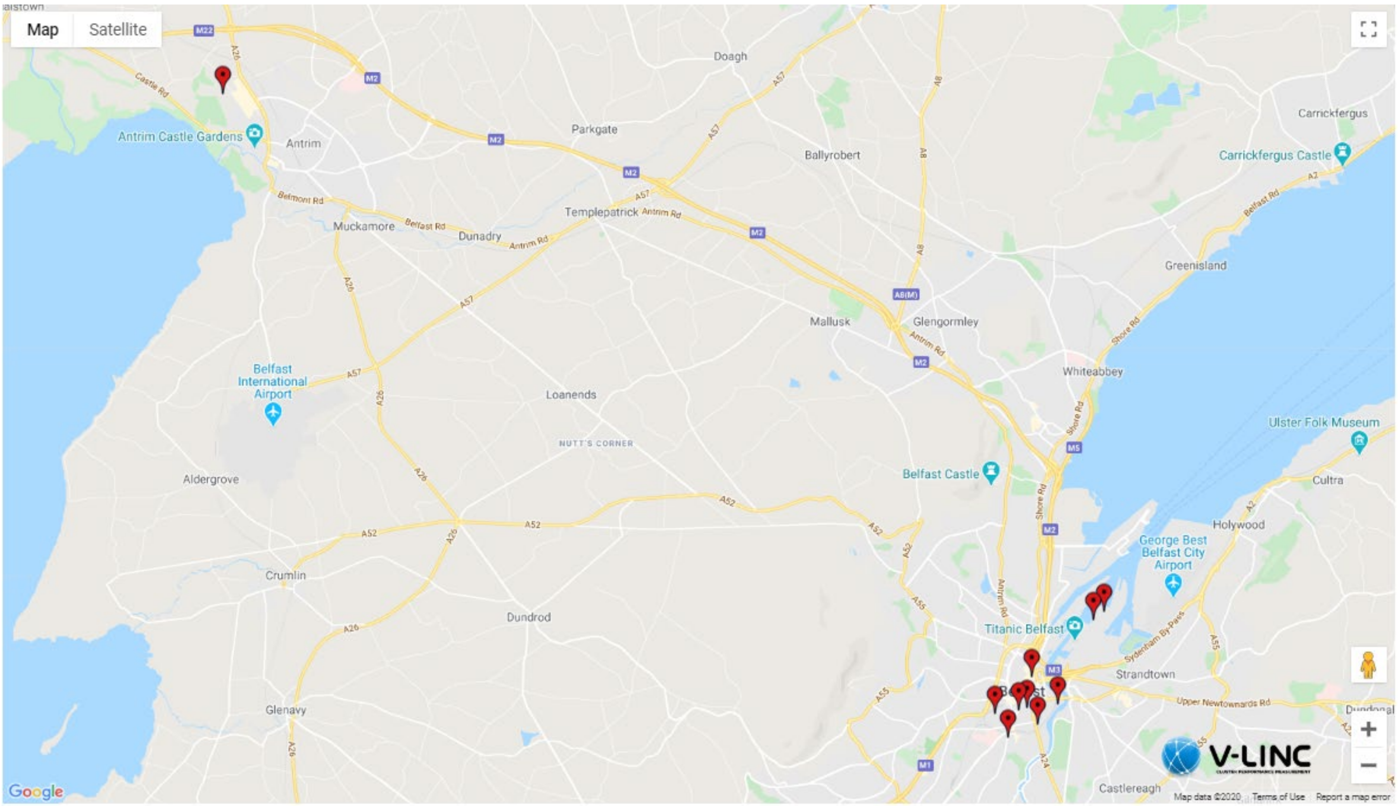


Figure 3: Map of the Respondent Firm Group – Office Locations in Northern Ireland

Linkage categories by geographic Scope:

In this study, Local linkages are those which occur within Northern Ireland; National linkages, are those outside of Northern Ireland and within the UK; European linkages are the connections outside of the UK; and International are all other linkages outside of Europe across the rest of the world. Table 2 and Figure 4 display the linkages reported at each geographic level for each of the eight linkage categories. Table 2 distinguishes the dominant geographic scope for each category and shows that 86% of Output linkages in this study are reported outside Northern Ireland, of which 23% is destined for the UK, a further 17% for the European marketplace and 46% internationally. Regarding Inputs, it is important to understand that the cyber security sector is predominantly service based, and the Inputs required to support such services primarily relate to other software or technical Inputs to build one's service. This can help to explain why 100% of Input linkages are reported at national, European and predominantly international (65%) scopes.

Geographic Scope	Local	National	European	International	Total (n)
GA - Government Agencies	55%	41%	5%	0%	22
IA - Industry Association	45%	45%	5%	5%	22
IN - Input	0%	15%	19%	65%	26
IP - Industry Peers	43%	21%	7%	29%	14
OU - Output	14%	23%	17%	46%	100
RD - Research & Development	73%	7%	7%	13%	15
SS - Specialist Service	83%	9%	0%	9%	23
TN - Training	31%	31%	14%	24%	29
Total (n)	81	61	30	79	251
Total (%)	32%	24%	12%	31%	

Table 2: Distribution of Linkage Categories by Geographic Scope

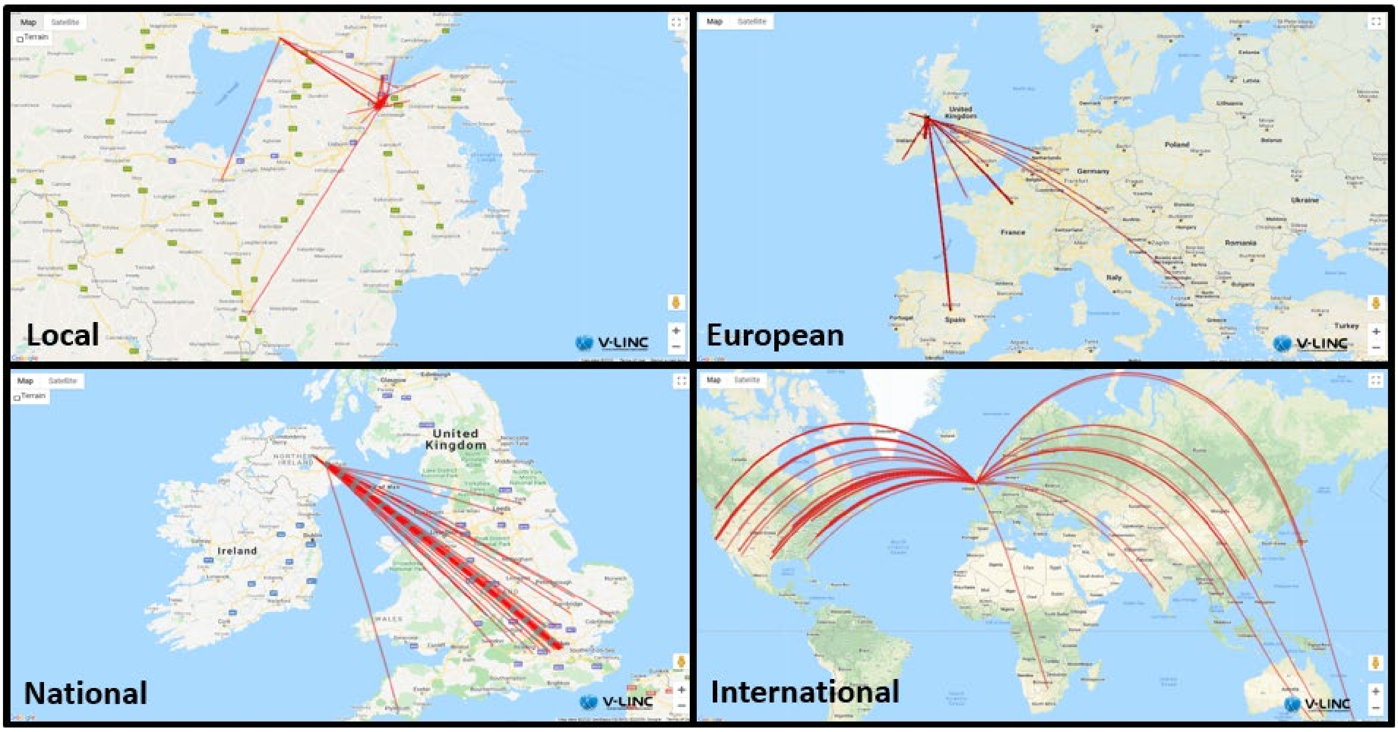


Figure 4: NI Cyber Linkages by Geographic Scope.

Porter (1998b) places great emphasis on linkages to and support from organisations and businesses, within the locality. The word local or locally appears in each element of his diamond of local industrial clustering. If local linkages are critical to the functioning of a cluster, Table 2 shows that local linkages make up the largest proportion (32%) of all linkages reported in the study, the remaining 68% being divided between National (24%), European (12%) and international (31%) linkages.

Focusing on the local and national perspective, it is a positive to see that the cyber security RFG is most heavily connected locally in the area of Specialist Services (83%) and Research and Development (73%), suggesting that the local economy is benefiting through the provision of services to the sector. Nationally, it is interesting to see the high proportions of linkages in the Government Agencies (41%) and Industry Association (45%) categories.

When looking at Figure 4, the local linkage maps highlight the number of linkages in and around Belfast city center, across the Cathedral, Titanic, Queen's and Linen Quarters. Nationally, it seems there is a highway of connections between Belfast and London, the European linkages showcase links into the Republic of Ireland, Spain, France and Germany. Furthermore, Figure 4 showcases pockets of the US which are heavily linked to the Northern Ireland cyber security sector on the West - Seattle, Portland, San Francisco, Los Angeles and San Diego; centrally through Chicago, Kansas City, Dallas, Austin and Houston and on the East – New York, Boston, Philadelphia, Washington and Tampa. Further east, it is clear there are connections with India, China, Australia and New Zealand which showcase the truly international focus of the sector in Northern Ireland. The next section presents the business impact values for each category.

Business Impact Findings

Tables 3a to 3e show the percentage of linkages (by category) that fall into the business impact bands. The business impact of each linkage category relates to the business importance of individual linkages based on the perception of expert respondents involved with these linkages. Table 3a shows the combined business impact results for all linkages, whilst tables 3b to 3e, break the data into Local, National, European and International linkages.

In table 3a, it is apparent that the results of the V-LINC analysis indicate that Outputs (59%) are rated of highest impact by respondents, followed by Training (42%) and Inputs (38%). As a company's customers and suppliers are central to the success of the firm this is not surprising. In all linkage categories, the majority of linkages are in the top two business impact bands (e.g. High and Medium bands); overall 85% of all linkages reported were in these bands. Industry Association linkages are rated of least importance to the firms with 27% of linkages in the Low (18%) and Tenuous (9%) categories.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	**>30 to 40**	23%	23%	38%	14%	59%	27%	4%	42%	**98**
Medium	**>20 to 30**	68%	50%	50%	57%	35%	46%	70%	48%	**119**
Low	**>10 to 20**	9%	18%	12%	29%	6%	27%	26%	10%	**32**
Tenuous	**>1 to 10**	0%	9%	0%	0%	0%	0%	0%	0%	**2**
Total		**22**	**22**	**26**	**14**	**100**	**15**	**23**	**29**	**251**

Table 3a: Business Impact by Linkage Category

It is also interesting to assess the business impact accorded to linkages at each geographic scope. Table 3b focuses on the business impact of 81 local linkages in Northern Ireland – the most populous geographic scope. The most important linkages at the local level, i.e. most linkages reported in the High business impact bands, are Output (50%), Research (36%) and Training (33%) linkages. It's important to qualify these results with the fact that 14% of Output linkages (n=14), 73% of Research (n=11) and 31% of Training (n=9) are reported at local level. Most of the Specialist Service, Research & Development and Government Agency linkages are recorded with local organisations, the connections are relatively important to the firms with the majority of these linkages reported in the Medium band.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	**>30 to 40**	17%	10%	0%	0%	50%	36%	5%	33%	**18**
Medium	**>20 to 30**	75%	70%	0%	100%	43%	55%	63%	56%	**51**
Low	**>10 to 20**	8%	20%	0%	0%	7%	9%	32%	11%	**12**
Tenuous	**>1 to 10**	0%	0%	0%	0%	0%	0%	0%	0%	**0**
Total		**12**	**10**	**0**	**6**	**14**	**11**	**19**	**9**	**81**

Table 3b: Business Impact by Linkage Category - Local Linkages

Table 3c presents the business impact data for 61 linkages that occur across the UK (National Linkages), 80% of which are in the top two business impact quartiles. In contrast to the local linkages, a sharp contrast at a National level exists where 100% of Industry Peer and Research and Development linkages are reported in the Low business impact band.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	**>30 to 40**	33%	30%	25%	0%	61%	0%	0%	33%	**24**
Medium	**>20 to 30**	56%	40%	50%	0%	30%	0%	100%	56%	**25**
Low	**>10 to 20**	11%	20%	25%	100%	9%	100%	0%	11%	**11**
Tenuous	**>1 to 10**	0%	10%	0%	0%	0%	0%	0%	0%	**1**
Total		**9**	**10**	**4**	**3**	**23**	**1**	**2**	**9**	**61**

Table 3c: Business Impact by Linkage Category – National Linkages

Surprisingly, the European linkages represent the least populous geographic scope. The business impact of the 30 linkages are displayed in Table 3d, 93% of which are reported to be of High or Medium business impact. Approximately 75% of all European linkages are reported across the value chain - Input and Output linkages. Training linkages are reported to be quite strong at this geographic scope.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	**>30 to 40**	0%	100%	60%	0%	53%	0%	0%	75%	**16**
Medium	**>20 to 30**	100%	0%	40%	100%	41%	0%	0%	25%	**12**
Low	**>10 to 20**	0%	0%	0%	0%	6%	100%	0%	0%	**2**
Tenuous	**>1 to 10**	0%	0%	0%	0%	0%	0%	0%	0%	**0**
Total		**1**	**1**	**5**	**1**	**17**	**1**	**0**	**4**	**30**

Table 3d: Business Impact by Linkage Category - European Linkages

Table 3e reports business impact for the 79 international linkages. Approximately 80% of the international linkages are made up of the value chain - Output and Input categories, in which most linkages are reported in the High band. Output and Input connections are focused on North America, Australia and Asia. International links with Training providers are also viewed as important to the respondent firms, with 86% in the High and Medium bands.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	**>30 to 40**	0%	0%	35%	50%	63%	0%	0%	43%	**40**
Medium	**>20 to 30**	0%	0%	53%	25%	33%	50%	100%	43%	**31**
Low	**>10 to 20**	0%	0%	12%	25%	4%	50%	0%	14%	**7**
Tenuous	**>1 to 10**	0%	100%	0%	0%	0%	0%	0%	0%	**1**
Total		**0**	**1**	**17**	**4**	**46**	**2**	**2**	**7**	**79**

Table 3e: Business Impact by Linkage Category – International Linkages

Table 4 reports the number and percentage of linkages reported in each of the business impact bands for each geographic scope, to compare the overall business impact of linkages at each geographic scope. Porter (2000) believes 'once a cluster forms, the whole group of industries becomes mutually supporting. Benefits flow forward, backward, and horizontally,' therefore, it is important to look closely at the business impact of local linkages. Local linkages account for 81 of the 251 reported, showcasing that respondent firms engage in more linkages across Northern Ireland (n=81) than at any other geographic scope. Only 22% (n=18) of which are reported as Highly impactful; however, this is the lowest proportion of linkages reported in the High business impact band when compared with National (39%), European (53%) and International (51%) scopes.

Respondents seem least likely to engage in European linkages, the results of which are confusing as Table 4 shows from a business impact perspective these linkages are valued more than the other geographic scopes, but this is reported as the least numerous scope. It seems from the results that the cyber sector in Northern Ireland is focused on the national market in the UK and the international market – predominantly the US.

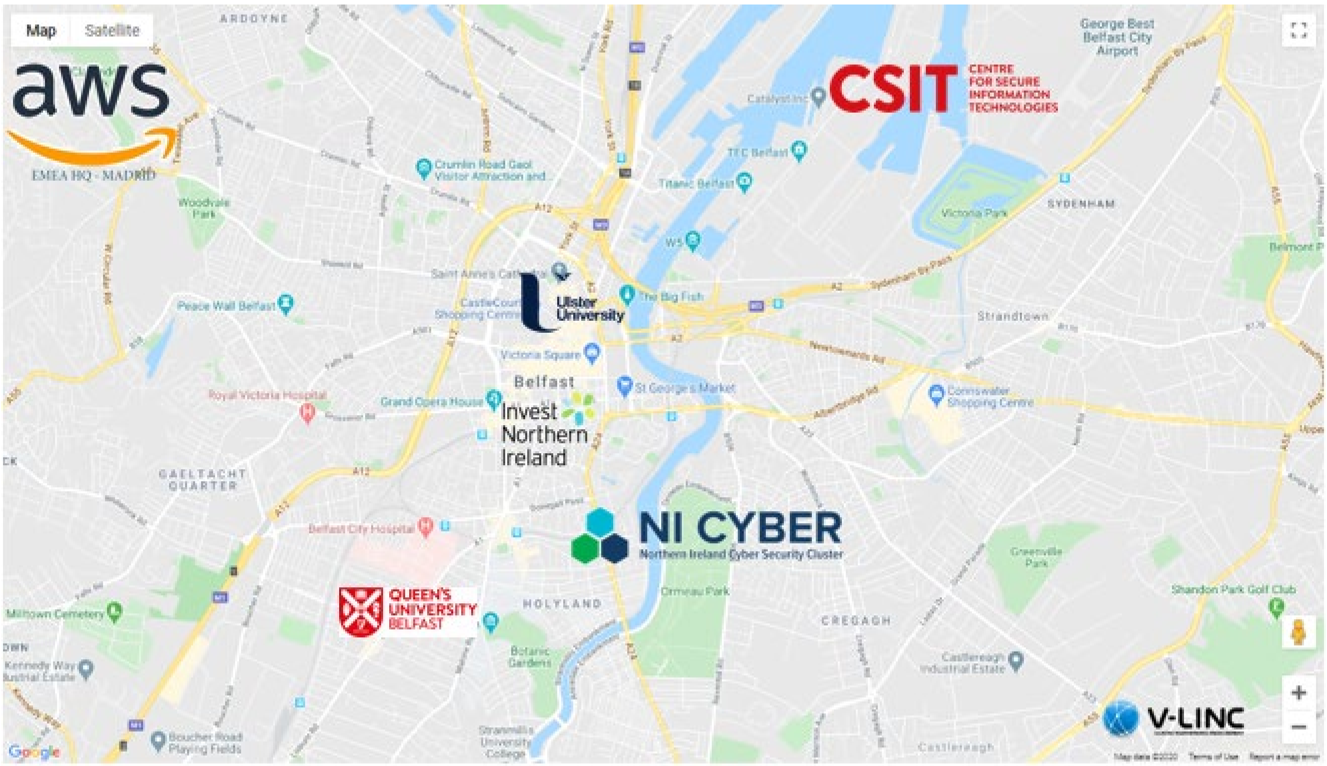
Geographic Scope		Local	National	European	International	Total
Business Impact						
High	**>30 to 40**	22%	39%	53%	51%	98
Medium	**>20 to 30**	63%	41%	40%	39%	118
Low	**>10 to 20**	15%	18%	7%	9%	33
Tenuous	**>1 to 10**	0%	2%	0%	1%	2
Percentage		32%	24%	12%	31%	100%
Total (n)		81	61	30	79	251

Table 4: Business Impact by Geographic Scope of Linkages

Key Connectors

Figure 5 illustrates the key connectors in the Northern Ireland Cyber sector. The key connectors are those organisations who connect the cluster. They are identified through the number of linkages they have with respondent firms and the importance of those linkages to respondents is reported in Table 5.

In terms of the key connectors identified in the cyber security sector in Northern Ireland, there are strong linkages to Industry Associations, Government Agencies and Research and teaching institutions. The standout Industry Association and Government Agency linkages for the RFG are with NI Cyber and Invest Northern Ireland who are connecting to all the respondents, with the majority of linkages to the organisations in the High and Medium bands.



aws
EMEA HQ - MADRID
CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES
Ulster University
Invest Northern Ireland
Belfast
NI CYBER
Northern Ireland Cyber Security Cluster
QUEEN'S UNIVERSITY BELFAST
V-LINC
Map
Satellite
Google

Figure 5: Key Connectors Northern Ireland Cyber Security Sector.

Key Connector		NI Cyber	Invest NI	CSIT	AWS Madrid	QUB	UU
High	**>30 to 40**	9%	20%	63%	75%	0%	0%
Medium	**>20 to 30**	73%	70%	38%	25%	67%	100%
Low	**>10 to 20**	18%	10%	0%	0%	33%	0%
Tenuous	**>1 to 10**	0%	0%	0%	0%	0%	0%
Total (n)		**11**	**10**	**8**	**4**	**3**	**3**
Linkage Category		10 IA, 1 RD	10 GA	6 RD, 1 TN, 1 SS	3 IN, 1 TN	1 TN, 1 OU, 1 RD	2 RD, 1 TN

Table 5: Business Impact of Key Connectors Northern Ireland Cyber Security Sector.

The Centre for Secure Information Technologies (CSIT), is the next most connected entity to the RFG – and their linkages to the cohort of firms extend across Research, Training and Specialist Service linkages. The RFG strongly value them with 63% of their connections being reported in the High business impact band. Other key connectors are difficult to find, with the analysis of the respondent companies only identifying three other organisations with whom three or more connections are made. These are Amazon Web Services (through their EMEA HQ in Madrid) linked to the RFG as a key Input and Training resource. Whilst Queens University Belfast (QUB) and University of Ulster (UU) are also connected to the RFG through Research, Training and Output linkages.

Policy Recommendations

Having reviewed the Cyber Security: A Strategic Framework for Action 2017-2021[4] and UK National Cyber Security Strategy 2016-2020[5] in tandem with the results of the V-LINC analysis, the following policies aim to develop the Northern Ireland cyber security sector.

1. Further develop and support NI Cyber as a cluster organisation with responsibility for the cyber sector in Northern Ireland.

The researchers propose further development and supports for the NI Cyber cluster organisation with the responsibility of supporting and facilitating the growth of the cyber sector in Northern Ireland. This would require the provision of financial supports to develop a fully functioning European style cluster organisation. The rationale for same is that Table 5 and Figure 5 show that NI Cyber is connected to each of the respondents who participated in this analysis piece – furthermore it is the only Industry Association which all the respondent firms are connected to in Northern Ireland (Table 3b). As such NI Cyber is the conduit connecting participants with others across cyber in Northern Ireland (Figure 6).

If national government through the Cyber Security: A Strategic Framework for Action 2017-2021 are focused on delivering "over 5,000 jobs by 2026 in this highly specialised area of cyber security" (page 11) and "the development of a world class cyber cluster" (page 12).

Consideration of strategic supports through an organisation whose agenda is not linked to any one organisation or institution – but industry-driven, university-fuelled, and government-supported may be relevant. ICN (2014) suggest that a cluster organisation can have a significant influence on strengthening collaboration in a cluster, through implementation of effective innovation policy. This report suggests respondent firms see value in connection with NI Cyber (Table 5) even though the cluster is at an early stage.

Whilst a national framework or Cluster Policy does not exist across the UK, it is important to note that supports for collaborative growth programmes[6] are available through Invest NI. In the context of the Cyber Security: A Strategic Framework for Action 2017-2021 and Cluster Policy in Northern Ireland report (Hetherington, Magennis and Victor, 2019), a government level discussion is required to discuss how NI Cyber could be further supported to deliver additionality and value for members across the triple helix.

[4] https://www.finance-ni.gov.uk/sites/CSSF2017-2021.pdf
[5] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[6] https://www.investni.com/collaborative-growth-programme

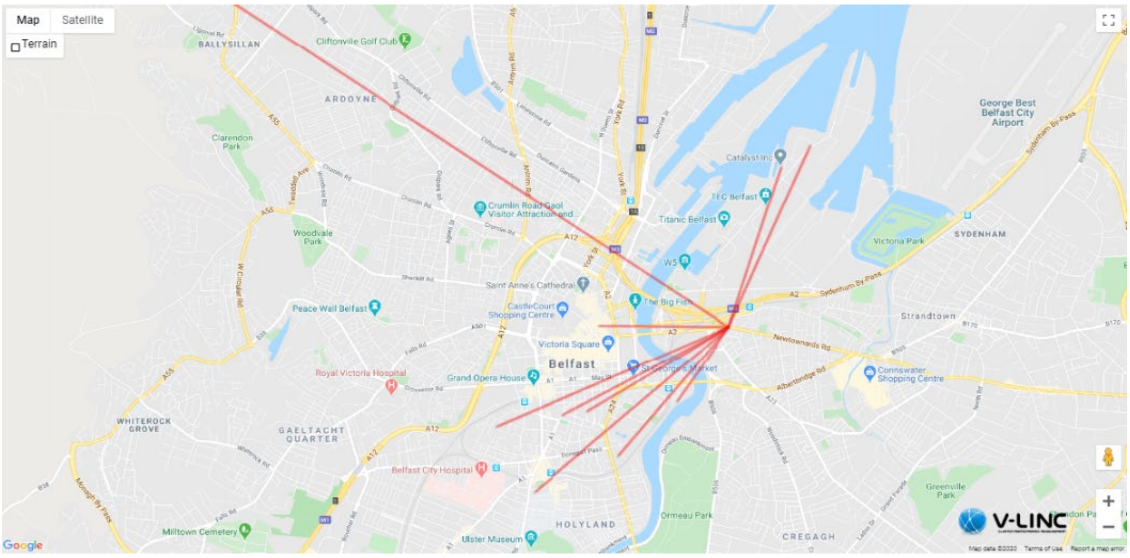


Figure 6: Local Industry Association linkages in the cyber security sector.

If supported and implemented correctly there is an opportunity for NI Cyber to connect and deliver on the four key thematic working areas of a cluster: (1) research and innovation, (2) internationalisation, (3) business development & marketing, (4) skills & training.

Key to delivering on these thematic working areas is financial support and time. To deliver a functioning cyber security cluster, international best practice in cluster development indicates that a 24-month funded period is required, e.g. as is the case in the Catalonia Cluster Development Strategy (Figure 7), and model used by Business Upper Austria. After the 24-months, the cluster is expected to fund itself through a combination of a smaller proportion of public funding, increased private funding and competitively won European and national funding.

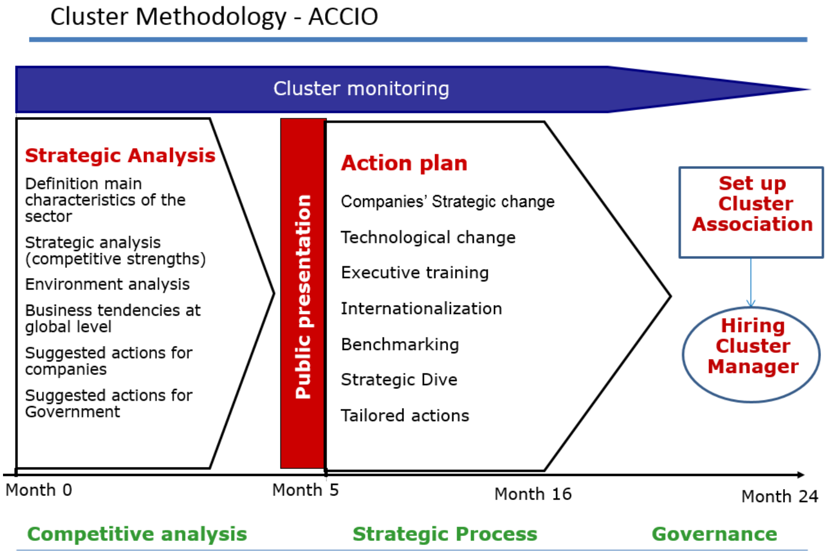


Figure 7: The Catalonia Cluster Development Strategy process utilised by ACCIÓ[7].

[7] Cluster Development Strategy by Joan Martí Estévez, ACCIÓ, Catalan Agency for Competitiveness @ Cluster Seminar Series in CIT, 09/15.

2. Prioritising facilitation of B2B and academic Research and Development linkages.

The authors believe there is a need to assist firms operating in the cyber security sector in Northern Ireland, to innovate and develop through increased R&D activity not only with academia and research institutions, but also through industry collaborations. R&D linkages were the 2nd least frequent linkage category in the study, with just 15 linkages reported – these linkages are a mixture of research centres and academic institutions. Significantly, 11 of these R&D linkages are reported locally in Northern Ireland, all but three of these are with CSIT. The others are with Universities locally (Table 2 and Figure 8).

In the Cyber Security: A Strategic Framework for Action 2017-2021 policy, Northern Ireland seeks to "be one of the world's leading cyber economies, delivering a thriving knowledge economy, due to exemplary talent; pioneering research and innovation; and the secure and resilient infrastructures needed to support businesses and safeguard the public." whilst "developing a culture of ongoing training, awareness and being alert to potential threats are all vital aspects to maintaining resilience, particularly as cyber threats escalate and are becoming even more complex."

Linked to the low numbers of R&D linkages reported by the respondents, Training is another category where industry connects with academia. There are only 9 Training linkages reported locally, of which 3 are with the local universities and colleges: Belfast Metropolitan College, Queens University Belfast and University of Ulster. It is apparent from the results that there is a preference for connecting with industry in terms of Training. When we consider R&D and Training linkages together, this suggests that industry find it challenging to connect with the universities and colleges. This is a problem that may be limiting firms in addressing the skills gaps required to expand the cyber talent pool and innovating in partnership with the academic institutes locally. There is a role here also for NI Cyber to become a bridge between firms and academic institutes to seek more appropriate mechanisms to build further connections and partnerships.

The UK has recently published their 'Cyber Security Skills in the UK Labour Market' report (DCMS, 2020) that explores the nature and extent of cyber security skills gaps (people lacking appropriate skills) and skills shortages (a lack of people available to work in cyber security job roles) using a mixture of: (1) Representative surveys with cyber sector businesses and the wider population of UK organisations, (2) Qualitative research with training providers, cyber firms and large organisations in various sectors, and (3) A secondary analysis of cyber security job postings on the Burning Glass Technologies database.

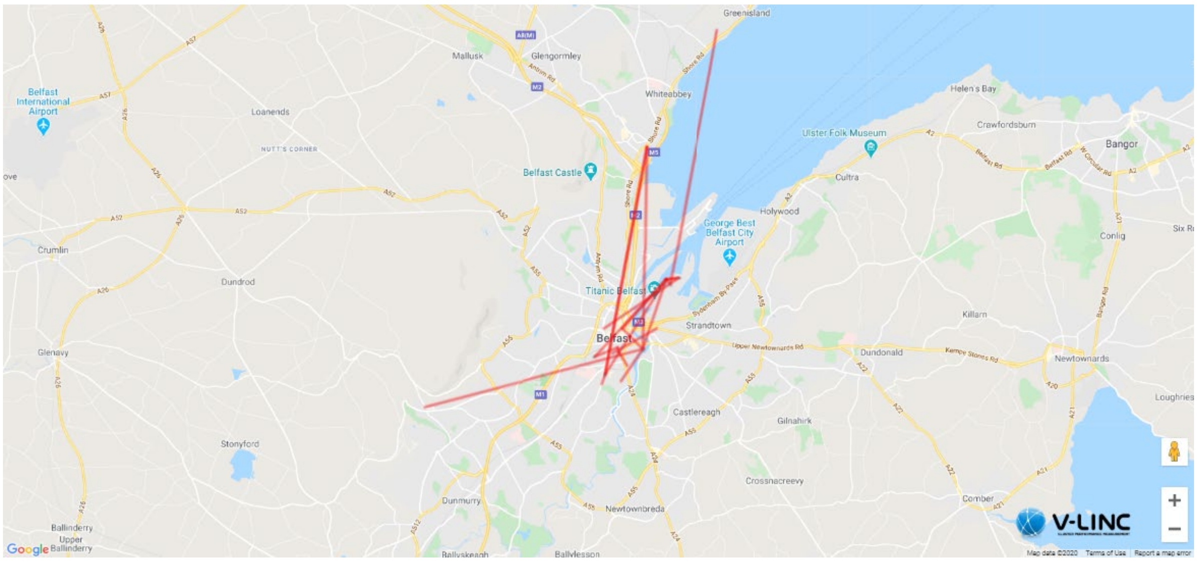


Figure 8: Local Research & Development and Training linkages in cyber security Northern Ireland.

Focusing back on R&D, another element that is concerning from the results is that there are no business to business R&D linkages between industry in Northern Ireland. This is an area that needs some attention. Developing funded co-operation projects between cyber focused firms, and firms from other sectors, in Northern Ireland can stimulate increased R&D linkages and innovation. An example of a best practice is the European co-operation project programme is used in Business Upper Austria. Co-operation projects have been used by the region since 1998 and have proven to be an effective and efficient method for SMEs to strategically differentiate themselves (TMG, 2014). To be eligible for government funding, a minimum of three companies participate in the project and at least one of those should be an SME.

Results from Business Upper Austria show that: 77% of firms continue to co-operate after projects end; 89% of the projects either would not have been realised without subsidies or would have had significantly lower expectations. Firms discover that pooling competencies enable firms to overcome barriers, such as limited funding, lack of management resources and technological competencies. Such programmes train SMEs to undertake larger R&D projects at national and European levels.

The Business Upper Austria R&D co-operation project model, facilitated by the NI Cyber cluster organisation in Northern Ireland, may be the conduit needed for realising more B2B market focused connections and opening further connections internationally for the sector.

Further opportunities for R&D connections are available via the US-Ireland R&D Partnership to address crucial technological research questions, and generate valuable discoveries and innovations, transferrable to the marketplace. From early 2020, Cybersecurity is the newest priority area to be funded under the partnership. NI Cyber could connect academics with industry locally, and through the Department for the Economy in Northern Ireland utilise the US-Ireland R&D Partnership to develop connections with scientists and engineers across the three jurisdictions to increase level of collaborative R&D. Each jurisdiction supports its own research costs, via Department for the Economy in Northern Ireland, Science Foundation Ireland (SFI) in Ireland and National Science Foundation (NSF) in the US.

As R&D is a key priority for clustering, further opportunities exist for NI Cyber and Cyber Ireland to collaborate, perhaps through the InterTradeIreland Synergy programme which aims to bring people together to find a common pathway to solve shared problems. The pathways available could be a combination of ITI supports, including linking with external partners, or purely providing an event for cross border groups to network and discuss where they could collaborate.

3. Facilitate and Focus on the Internationalisation of Micro and SME Cyber Firms.

The Cyber Security: A Strategic Framework for Action 2017-2021 policy in Northern Ireland suggests that the region "has a growing reputation as a region of expertise and knowledge in cyber security – not only within the UK, but internationally. It is a business sector which is expected to grow exponentially and with the right physical and digital infrastructures in place, world class research and the right talent pool available, we can capitalise on international opportunities."

As noted previously, the cyber security sector in Northern Ireland employs almost 1,700 people across 75 companies (Computer Weekly, 2019). There is an ambitious target of having 5,000 employees in the sector by 2030 (NDNA, 2020). This cohort of companies is predominantly SMEs in Northern Ireland whom have built upon expertise in developing cyber security products and services in the areas of: Cyber Professional Services, Threat Intelligence, Monitoring, Detection and Analysis, Endpoint Security (including Mobile). Expertise in emerging sub-sectors such as IoT Security, SCADA and ICS, Post-Quantum Cryptography is developing rapidly (DCMS, 2020).

Of the ten firms in the respondent firm group (Table 1), six of these are Micro or SMEs (Figure 9). These firms account for 40% of the European and International Output linkages in the study, this is a testament to the programmes and supports provided by Invest NI in direct support to such SMEs.

There are a number of roles that NI Cyber could play regarding the provision of opportunities between members of NI Cyber, to collaborate and service the international market further. There is an opportunity to connect the MNC and Indigenous cyber industry in Northern Ireland through ‘cyber brokerage’ events. These could take a number of formats – connecting MNC and Indigenous cyber firms to 1) trade with each other and/or 2) for the MNC to mentor SMEs or micro enterprises on expanding internationally and collaborating with Invest NI to reach new markets.

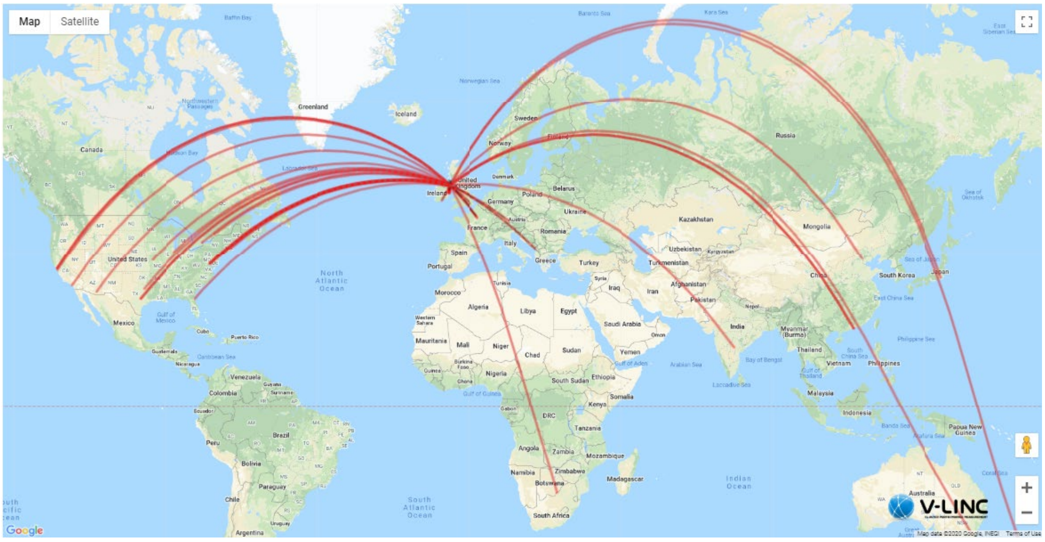


Figure 9: European & International Output Linkages of Micro and SME Cyber Firms in Northern Ireland.

Furthermore, NI Cyber through its collaboration with the Cork Institute of Technology are able to be able to facilitate the creation of linkages and partnerships with CyberForum’sP8F[8]P Business Roaming Agreement. The Business Roaming Agreement (BRA) http://clusterize.org/ is a service provided by the German cyber cluster - CyberForum. Clusters sign up to the BRA to provide their facilities and office space as a soft-landing platform for member firms of other clusters to utilise when visiting their region, to develop markets or research connections for their firm. In exchange the host cluster’s member firms can utilise the facilities and hot desk in the offices of other clusters who sign the BRA. Fifty-seven locations in 32 different countries are available. Perhaps CSIT, UU or Invest NI would be able to sign this agreement to bring benefits to NI Cyber participating firms in terms of soft landing for internationalisation.

[8] Cyberforum is the largest high-tech cluster in Germany with over 1000 members https://www.cyberforum.de/

To kick start soft-landing opportunities perhaps the InterTradeIreland Synergy programme could be leveraged to support the bringing together of companies interested in developing connections from both Ireland and Northern Ireland to develop more cross-border trade. The Memorandum of Understanding signed between the Department for the Economy NI and the State of Maryland Departments of Commerce and Labor to formalise their commitment to supporting cross collaboration and growth of the cyber security sector in October 2019 – could also be used as a template for soft-landing also.

Closing Remarks

This paper has described and applied the V-LINC methodology for identifying and analysing the linkages that cyber security firms in Northern Ireland engage in. If NI Cyber is to support and formalise the success of the sector through growth and expansion in the global marketplace, change is required to address the problems and opportunities identified. The analysis shows evidence of fledgling research, development and innovation linkages, however if a fully functioning cluster is to develop, which will have further impacts on economic growth as called for by NDNA (2020), there is a need for increased competition and co-opetition. Skills requirements will need to be addressed for the sector to ensure a flow of talent exists to drive and nurture the sector.

Northern Ireland needs to strategically strengthen and expand the cyber security sector. To do so it is imperative that its firms are linked more vigorously with international markets. Internationalisation based on solid supports is critical in this regard. The formalizing of the NI Cyber cluster organisation to work with and support members can be invaluable as firms are seeking to grow and expand.

A common theme for clusters – even well-established ones – is that they have a robust governance system, are highly organised, and meet many of their initial stated goals. Yet, a network analysis can reveal that while local ties are plentiful, other collaborations may be outsourced to other regions or countries. The success of a cluster can oftentimes mask its weaknesses, but it is by learning this information that interventions can target these particular shortcomings. In this example, improving the quality of connections with local knowledge institutions within the cluster and increasing collaborative projects between academia and industry will strengthen the overall cluster and begin to address the skills gap.

NI Cyber need to develop a longer-term strategic perspective, as they seek to develop into a European Style Cluster organisation. Core funding is imperative as the cluster concept needs to be showcased and proven to industry – a combination of both Phase 2 Collaborative Growth Programme funding from Invest Northern Ireland and dedicated cluster funding from the Department of Economy, Northern Ireland would be transformative for the organisation. Future research may analyse the long-term funding model for a proposed cluster organisation, in European regions public financing is available to supporting a cluster organisation in its first 2-3 years of existence (CEBR, 2014; ECO, 2013; Byrne, 2016). The NI Cyber cluster organisation should look towards a model of self-financing or a mixture of public and private financing through the provision of activities and services to members into the future.

References

- Byrne, E. (2016), 'Incorporating network theory and visualisation in cluster analysis: A hybrid methodology applied to European ICT clusters,' PhD Thesis, Cork Institute of Technology.
- Business Upper Austria (2014) 'Cluster & Network Cooperation Projects', Accessed on 17th of August, Available online @ http://www.clusterland.at.
- Computer Weekly (2019) 'Northern Ireland generating cyber security knowledge and jobs.' By Warwick Ashford, May. Available Online @ https://www.computerweekly.com/news/252463046/Northern-Ireland-generating-cyber-security-knowledge-and-jobs.
- DCMS (2020), 'UK Cyber Security Sectoral Analysis 2020, Published by Department for Digital, Culture, Media and Sport, March. Available Online @ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957960/UK_Cyber_Sectoral_Analysis__2020__Report_V2.pdf.
- Digital Catapult, (2019), 'Accelerating the Early Adoption of Advanced Digital Technologies Across the UK: Annual Engagement & Impact Report,' Available Online @ https://assets.ctfassets.net/nubxhjiwc091/1b3yiumNBabpL0UWrcuY58/f73d10282daaa9d8823ceebec8b04543/Digital_Catapult-AR2019_webready.pdf
- ECO (2013), 'European Cluster Excellence Scoreboard: Pilot Version,' European Cluster observatory, on behalf of the Enterprise and Industry Directorate-General of the European Commission. September, Available online @ www.emergingindustries.eu.

- fDi Markets Intelligence (2020), 'Digital Economies of the Future 2019/20 – the results.' Available Online @ https://www.fdiintelligence.com/Digital-Economies.
- Hobbs, J. (2010), A Framework for the Analysis of Spatial Specialisations of Industry, PhD thesis, Cork Institute of Technology, Cork.
- Hobbs, J., and Byrne, E., (2014), Cluster Organisation and Finance, Presented at the Cork County Council Cluster Development & Collaboration Workshop, October 10th, Bord Iascaigh Mhara Clonakilty, Cork.

- ICN (2014), ‘Why Clusters,’ International Cleantech Network, Accessed on 10th August, Available online @ http://internationalcleantechnetwork.com.
- NDNA, (2020), New Decade New Approach. The Tánaiste and Secretary of State for Northern Ireland have published the text of a deal to restore devolved government in Northern Ireland, 9th January. Available online @ https://www.dfa.ie/media/dfa/newsmedia/pressrelease/New-Decade-New-Approach.pdf.
- Porter, M. E. (1990), The Competitive Advantage of Nations, New York, Free Press.
- Porter, M. E. (1998a), ‘Clusters and the new economics of competition’, Harvard Business Review 6, 77–90.
- Porter, M. E. (1998b), On Competition, Harvard Business School Press.
- Porter, M. E. (2000), The Oxford Handbook of Economic Geography, Oxford University Press.
- TMG (2014), ‘Strategic Programmes in Upper Austria,’ The TMG Group - Upper Austria's Business Agency. Available online @ https://www.biz-up.at/kooperation/unserecluster
- McKee, R. (2019), NI battles for cyber-security jobs amid global shortage, BBC News NI, 23 December. Available Online @ https://www.bbc.com/news/uk-northern-ireland-50646395