A V-LINC Analysis of the Irish South West 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

Ireland is among the leading EU member states when it comes to uptake and use of digital technologies, it ranks 7 out of the 28 EU member states in the European Commission Digital Economy and Society Index (DESI, 2019). This indicates that the internet and technology are a significant part of the Irish lifestyle. Globally, the cyber security sector will be valued at $250 billion within five years and is rapidly evolving to tackle the $600 billion which high tech crime is costing governments, companies, and citizens around the world. Irish Tech News (2019) reports that Ireland has the world class potential to become a global cyber security centre of excellence, it's cyber security industry employs over 6,500 people and includes many of the world's top security software MNCs: McAfee, Trend Micro, Forcepoint, eSentire, and MasterCard, as well as a growing SME sector. 'However, there is a lack of understanding in relation to the needs and trajectory of the sector in Ireland and therefore, it is important that an analysis is conducted.

In order to carry out this analysis, V-LINC, a methodology that identifies, records and analyses the linkages that firms in clusters engage in, is applied to the concentration of the Cyber Security Sector in the South West of 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 South West 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 the South West of Ireland, and amongst 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.

This report was funded by InterTradeIreland.

Introduction

This paper represents a collaboration between the Cork Institute of Technology and Cyber Ireland who partnered to apply V-LINC to the Cyber Security specialisation in the South West of the country.

IDA Ireland (2018) believes Ireland's second city 'Cork' in the South West is a hidden gem for Cyber Security. There are close to 60 overseas technology companies in Cork, in manufacturing, software development and global business services. More than 1,000 people work in the Southern region (Cork and Kerry) either with pure-play cyber security companies or others with specific security teams. Trend Micro was the first pure-play security company to set up in Cork over 15 years ago, and now it employs over 250 people. McAfee employs more than 350 people at its Cork site, which includes a security operation centre and engineering team. Others in the region include Cylance, Malwarebytes, eSentire, JRI America, AT&T Security, Sophos, TransUnion, and Keeper Security. Since 2013, pure-play firms have announced 850 jobs in the South West.

The paper begins with an explanation of V-LINC, a methodology which records, categorises, 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 (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 Ireland and the South West, then reviews findings from V-LINC analysis on the linkages of a sample of cyber firms in the South West. 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, the paper closes with recommendations on how to strengthen and support Cyber Ireland.

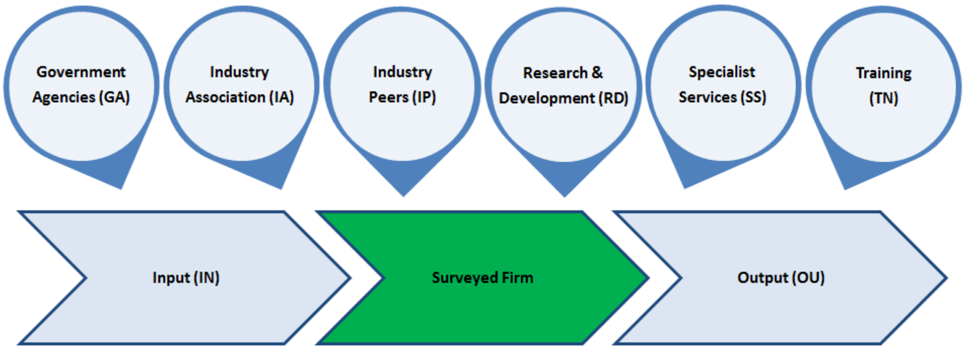


Figure 1: The Eight V-LINC linkage categories analysed for each firm.

The authors would like to acknowledge the contributions of Dr Eoin Byrne, Cluster Manager Cyber Ireland and Ronan Lenihan, IDA Ireland.

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. The 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 Ireland and the South West, in particular, 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).

The Cyber Security Sector in Ireland and it's South West

Due to the increasing threats of cyber-attacks to citizens, businesses, governments and critical national infrastructure alike, cyber security is a rapidly growing industry internationally. Ireland has a strong, internationally recognized cyber security cluster, made up of over 40 cyber security and security related MNCs, including five of the top ten worldwide security software companies, as well as over 60 indigenous SMEs. This sector covers the full spectrum of activities, including: Engineering - (threat research, SOC, QA/QC, dev, localisation, risk & compliance), Supply chain management, Multilingual tech support, and Shared services. Ireland's National Cyber Security Strategy 2019 – 2024 (Government of Ireland, 2019), showcases that the number of cyber security companies making Ireland their home continues to expand, along with employment levels - with nearly 6,500 cyber security professionals working in the nation, with significant potential for future growth.

Furthermore, many of the leading global technology companies have a significant presence in Ireland (e.g. Google, Apple, Amazon, IBM, Microsoft) and over the last 20 years the country has established itself as "The Data Capital of Europe"; Dublin is now the leading destination for data hosting facilities in Europe, with 25% market share of the European data market.[2] Although Ireland is a relatively small country, it has a large role to play regarding data, cyber security and international cyber policy. Ireland's second largest city, Cork, located in the South West of the country is home to companies like; AT&T Security, Cylance, eSentire, FireEye, Forcepoint, Keeper Security, Malwarebytes, McAfee, Sophos, Smarttech, Trend Micro, and TransUnion. The city of Cork is home to nearly 60 technology companies involved in manufacturing, software development and global business services. In addition to this, several companies are growing their cyber security teams internally. Companies like IBM, Clearstream, Johnson Controls, VMware, Qualcomm, Apple, Amazon, Dell EMC, Inhance, and McKesson are all developing in-house cyber security teams.

As well as the strong MNC sector in Ireland, the educated workforce and research capabilities have been sited as strengths that have led to the development of the sector. Ireland has one of the highest graduate rates in the mathematics, science and technology field within the EU (Eurostat, 2016). Ireland's Higher Education Institutes are very aware of the importance of Cyber Security in today's digitally driven society. The "collaboration culture" that exists here between industry leaders, research centres, and academia enables Ireland to develop as a world-class Cyber Security practice and innovation hub.

[2] Host In Ireland Quarter 4 2018 Report, available at: http://hostinireland.com/dataindustryreportq42018/

The cyber security talent pool in Ireland is fed by a supply of graduates from four undergraduate degree courses in cyber security, sixteen postgraduate degree courses with modules in Cyber and eight postgraduate degree courses in cyber security. The Cyber Security Skills Initiative, launched by Technology Ireland ICT Skillnet in October 2018, is a comprehensive plan to train 5,000 people in 4,000 companies, in cyber security skills, to tackle the issue, by providing cross and upskilling opportunities for IT operatives across all sectors to a recognised standard. This allows them to act as cyber security officers for their organisations, thereby raising the general level of protection across the country. Additionally, a Cyber Security Apprenticeship programme is being piloted in Cork & Dublin in 2019/2020 by Fast Track into Information Technology. The apprenticeship is a 2-year programme which involves completion of 4 - six-month long semesters. Although there is a broad range of programmes delivering a talent pipeline, there is still a skills shortage identified by the cyber security industry in Ireland.

Cyber security research in Ireland is dispersed across a number of the academic institutes and national research centres. For example across the academic institutes, there is: UCD Centre for Cyber security and Cyber crime Investigation (Cybercrime & Fraud Analysis), Cork Institute of Technology (Threat Detection & Networks), UCC Computer Science Centre (IT Security & Cryptography), University of Limerick Data-Comm Security Laboratory (IT Security & Cryptography), National University of Ireland Galway (M2M Security). In the Science Foundation Ireland National Research Centres, there is security research applied to Software Engineering (LERO), Data Analytics (INSIGHT), Future Networks (CONNECT), and Smart Manufacturing (Confirm). However, a difficulty of the current research landscape is that there is no dedicated national cyber security research centre, which makes it difficult for the industry to engage with academia and a lack of a national co-ordinated approach to cyber security research.

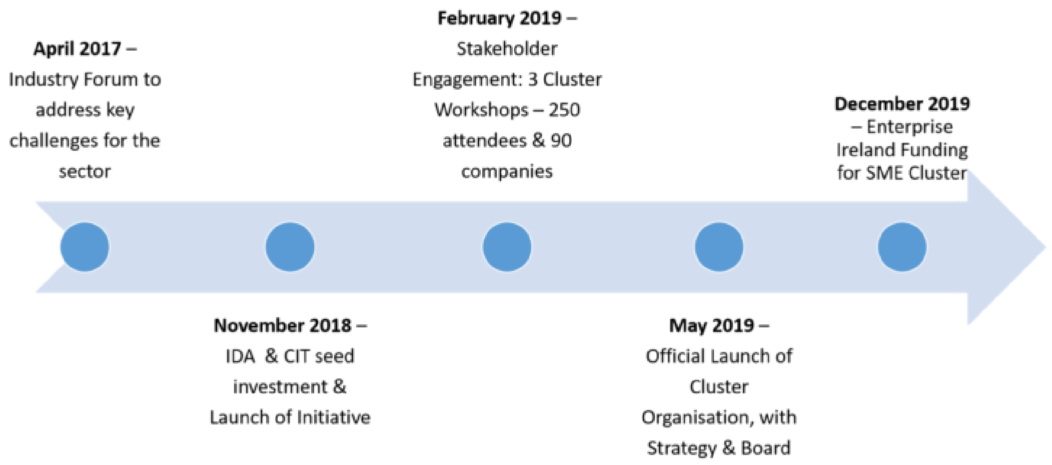
From a national Government perspective, the National Cyber Security Centre (NCSC) was established in 2011 as the operational unit of Government regarding network and information security. The role of the NCSC is to lead in the management of major cyber security incidents, provide guidance and advice to citizens and businesses, and manage cyber security related risks to key services. The key objectives of Ireland’s National Cyber Security Strategy 2019 – 2024 (Government of Ireland, 2019) are:

- To ensure Ireland’s cyber security readiness and respond to, and manage cyber security incidents, including those concerning national security.
- Protect and manage disruption of services involving critical national infrastructure from cyber-attacks.
- To further grow and develop the cyber security sector in Ireland and be cyber-ready.
- To implement the best technology and measures available internationally in Irish businesses.
- To increase awareness and develop skills among organisations and individuals around cyber security.

Locally in the South West, over the past ten years, the Department of Computer Science, at Cork Institute of Technology (CIT), have developed a suite of programmes with information security as a central pillar. Several companies who have established security operations in Cork have referenced, that a key factor in their decision to locate here was the talent pipeline available at and postgraduate level in Computer Science at CIT. Recognising the opportunity to grow Ireland's cyber security sector and the need to address specific challenges for the sector, a number of well-placed technology and cyber security companies (SMEs and MNCs) and academic bodies, led by CIT, saw the value in collaboration to establish a national cyber security cluster.

Cyber Ireland, which is hosted at Cork Institute of Technology and supported by IDA Ireland and Enterprise Ireland, brings together industry, academia and government to represent the needs of the cyber security ecosystem in Ireland. It aims to enhance the innovation, growth and competitiveness of Ireland's cyber security ecosystem and has a number of objectives, developed by industry, including:

- **Building the Community** - Stronger Promotion & Supporting cross-industry collaboration
- **Talents & Skills** - Ensuring a sustainable pipeline of Cyber Security Talent
- **Research & Development -** Enhancing collaborative R&D between industry and academia.
- **Grow & Export** - Supporting Irish SMEs & Start-ups to grow and export globally from Ireland.



April 2017 – Industry Forum to address key challenges for the sector
November 2018 – IDA & CIT seed investment & Launch of Initiative
February 2019 – Stakeholder Engagement: 3 Cluster Workshops – 250 attendees & 90 companies
May 2019 – Official Launch of Cluster Organisation, with Strategy & Board
December 2019 – Enterprise Ireland Funding for SME Cluster

Figure 2: Cyber Ireland Development Timeline

Since the launch of Cyber Ireland in May 2019, to date there are over 170 member organisation, 140 of which are from industry. Furthermore, Cyber Ireland has been showcased as a model for good practice in cluster development in Ireland as part of the following strategies and programmes: Future Jobs Ireland 2019, South West regional Enterprise Plan to 2020, Regional Spatial & Economic Strategy (RSES) for the Southern Region, ecoRIS3 Interreg Europe Project, and ERASMUS+ International Credit Mobility.

This research has been funded by InterTradeIreland, as part of their mandate to connect firms across Ireland. The support of Dr Eoin Byrne, Cluster Manager, Cyber Ireland has been invaluable in organising interviews and connecting with the sector. V-LINC was applied to a sample of 11 cyber security firms in the South West. Thirteen face to face meetings were held with personnel from these companies to gather information on their key relationships. These meetings uncovered 379 firm linkages (Table 1). The term Respondent Firm Group (RFG) relates to the summation of data for the eleven cyber security respondent firms.

V-LINC Analysis Results: Cyber Security South West of Ireland.

Table 1 and Figure 3 showcase the firms and their respective size in the South West of Ireland who participated in the V-LINC analysis. It provides the percentage of linkages they report in each of the eight categories, along with the total number of links they engage in. It also distinguishes the total numbers of linkages per category for the RFG. Table 1 reports that the most frequent linkages are in Outputs, which account for 29% of linkages reported; followed by Industry Association (13%), Training (12%) and Specialist Services (12%). This is not unexpected, as firms exist due to the continued development of revenues and customers. Whilst, Specialist Services and Training feed into a Cyber firm's product and service offering, Industry Associations links may provide access to new customers. The least frequent linkage categories are Industry Peers (7%) and Government Agencies (8%). The low numbers of industry peer linkages may indicate difficulties in building trust-based collaborations with competitors, which Porter (1990, 1998b) highlights as essential in a cluster.

Company Name	Firm Size	GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
AT&T Cyber Security	Medium (50 - <250)	2%	2%	2%	9%	70%	4%	8%	4%	53
Cork Cyber Sec SME	Medium (50 - <250)	9%	18%	18%	0%	18%	0%	27%	9%	22
Cyberlink Security	Micro (<10)	11%	11%	5%	0%	47%	5%	16%	5%	19
eSentire	Medium (50 - <250)	6%	22%	11%	6%	28%	0%	17%	11%	18
JRI America	Medium (50 - <250)	9%	18%	14%	5%	14%	5%	14%	23%	22
McAfee	Large (250+)	2%	13%	7%	0%	29%	7%	29%	13%	45
McKesson	Large (250+)	13%	17%	13%	3%	13%	17%	3%	20%	30
Qualcomm	Medium (50 - <250)	7%	28%	10%	0%	10%	7%	0%	38%	29
Sophos	Small (<50)	3%	6%	39%	0%	39%	0%	8%	6%	36
Trend Micro	Large (250+)	19%	8%	3%	19%	19%	6%	11%	13%	62
UTRC	Medium (50 - <250)	7%	19%	0%	12%	16%	42%	5%	0%	43
RFG Average		8%	15%	11%	5%	28%	8%	12%	13%	34
Total (n)		**31**	**49**	**37**	**25**	**111**	**36**	**45**	**45**	**379**
Most Populous (Rank 1-8)		7th	2nd	5th	8th	1st	6th	3rd	3rd	

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

[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.

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."

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.

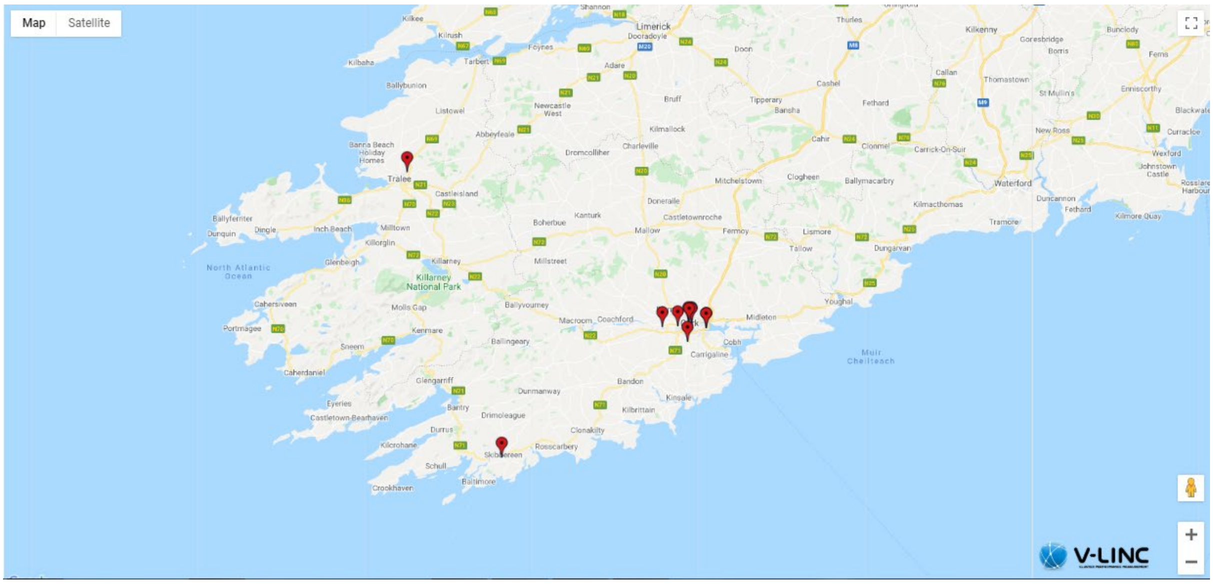


Figure 3: Map of the Respondent Firm Group – Office Locations in the South West of Ireland

Linkage categories by Geographic Scope:

In this study, Local linkages are those which occur within the South West region of the Republic of Ireland; National linkages, are those outside of the South West and within the Republic of Ireland; European linkages are the connections outside of the Republic of Ireland; 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 95% of Output linkages in this study are reported outside Ireland, of which 54% are destined for the European marketplace and 41% Internationally. 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.

Geographic Scope	Local	National	European	International	Total (n)
GA - Government Agencies	23%	52%	23%	3%	31
IA - Industry Association	65%	18%	12%	4%	49
IN - Input	14%	16%	27%	43%	37
IP - Industry Peers	0%	12%	56%	32%	25
OU - Output	2%	3%	54%	41%	111
RD - Research & Development	44%	14%	31%	11%	36
SS - Specialist Service	53%	22%	18%	7%	45
TN - Training	64%	16%	9%	11%	45
Total (n)	**115**	**60**	**120**	**84**	**379**
Total (%)	**30%**	**16%**	**32%**	**22%**	

Table 2: Distribution of Linkage Categories by Geographic Scope

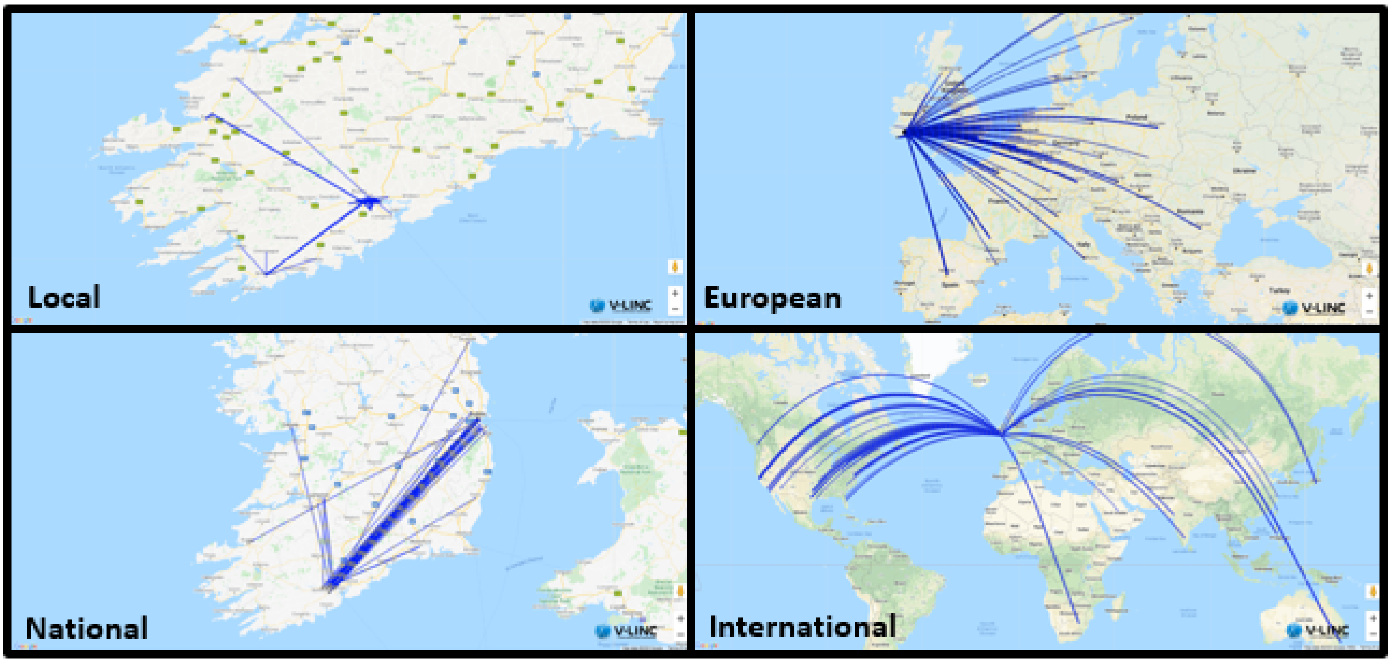


Figure 4: South West Cyber Linkages by Geographic Scope.

If local linkages are critical to the functioning of a cluster, Table 2 shows that Local linkages make up the second largest proportion (30%) of all linkages reported in the study, the remaining 70% being divided between National (16%), European (32%) and International (22%) linkages. However in contrast to the overall linkages in terms of just inputs, 100% of these linkages are reported at National, European and International scopes This might be as a result of the fact 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.

Additionally from a local perspective, it is a positive to see that the cyber security RFG is most heavily connected locally in the areas of Industry Association (65%), Training (64%), Specialist Services (53%) and Research and Development (44%), suggesting that the local economy is benefiting through the provision of services to the sector. Nationally, it is not unusual to see the high proportions of linkages in the Government Agencies (52%) category as Ireland is a centrally governed country.

When looking at Figure 4, the Local linkage maps highlight the number of linkages in and around Cork City while the companies located in more rural settings in West Cork and Kerry have good connections back into the city. Nationally, there is a highway of connections between Cork and Dublin, with several linkages destined for Limerick and Galway also. The European linkages showcase the plethora of connections across Europe and why this is the most populous geographic scope. We can see links across the UK and further afield into the Nordic countries, across Central Europe, into Eastern Europe (Poland, Romania etc.) and Southern Europe in Italy and Spain. Furthermore, Figure 4 showcases pockets of the US which are heavily linked to Ireland's South West cyber security sector on the West, centrally and on the East coast. Further east, it is clear there are connections with India, China, Australia and South Africa which showcase the truly international focus of the sector. 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, while tables 3b-3e, break the data into the individual geographic scopes.

In table 3a, it is apparent that the results of the V-LINC analysis indicate that Inputs (73%), Industry Peers (72%) and Outputs (63%) are rated of highest impact by respondents with the largest proportion of these linkages occurring in the 'High' business impact band. As a company's customers and suppliers are central to the success of the firm this is not surprising. In six out of the eight linkage categories, most linkages are in the top two business impact bands (e.g. High and Medium bands); overall 77% of all linkages reported were in these bands. Research and Development and Industry Association linkages are rated of least importance to the firms with 61% and 51% of linkages respectively in the Low and Tenuous categories.

Category		**GA**	**IA**	**IN**	**IP**	**OU**	**RD**	**SS**	**TN**	**Total (n)**
Business Impact										
High	**>30 to 40**	29%	14%	73%	72%	63%	8%	22%	18%	152
Medium	**>20 to 30**	52%	35%	22%	12%	36%	46%	53%	47%	140
Low	**>10 to 20**	19%	47%	5%	8%	1%	53%	24%	33%	79
Tenuous	**>1 to 10**	0%	4%	0%	8%	0%	8%	0%	2%	8
Total		**31**	**49**	**37**	**25**	**111**	**36**	**45**	**45**	**379**

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 115 local linkages in the South West of Ireland. The most important linkages at the local level, i.e. most linkages reported in the High and Medium business impact bands, are Output (100%), Government Agencies (100%), Input (80%) and Specialist Services (71%) linkages. It's important to qualify these results with the fact that 2% of Output linkages (n=2), 23% of Government Agencies (n=7), 14% of Input (n=5) and 53% of Specialist Services (n=24) are reported at local level. Most of the Training (64%), Specialist Service (53%) and Research and Development (44%) linkages are recorded with Local organisations, but are not viewed as important to the RFG with over 40% of these linkages reported in the Low and Tenuous bands. Research and Development stands out with 75% of linkages in these bands.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	>30 to 40	0%	6%	20%	0%	50%	0%	13%	17%	12
Medium	>20 to 30	100%	44%	60%	0%	50%	25%	58%	42%	55
Low	>10 to 20	0%	44%	20%	0%	0%	56%	29%	38%	42
Tenuous	>1 to 10	0%	6%	0%	0%	0%	19%	0%	3%	6
Total		7	32	5	0	2	16	24	29	115

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

Table 3c presents the business impact data for 60 linkages that occur across the Republic of Ireland, 70% of which are in the top two business impact quartiles. In contrast to the Local linkages, no tenuous National linkages exist. Whilst a larger proportion of Industry Association 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	25%	11%	50%	67%	50%	0%	30%	0%	15
Medium	>20 to 30	44%	22%	50%	0%	50%	60%	50%	71%	27
Low	>10 to 20	31%	67%	0%	33%	0%	40%	20%	29%	18
Tenuous	>1 to 10	0%	0%	0%	0%	0%	0%	0%	0%	0
Total		16	9	6	3	4	5	10	7	60

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

The European linkages represent the most populous geographic scope. The business impact of the 120 linkages are displayed in Table 3d, 85% of which are reported to be of High or Medium business impact. Approximately 63% of all European linkages are reported across the value chain, e.g. Input, Output and Specialist Service linkages in the High and Medium bands. Research and Development linkages are reported to be the weakest linkage category at this geographic scope.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	>30 to 40	57%	50%	90%	64%	77%	9%	13%	0%	73
Medium	>20 to 30	29%	0%	0%	14%	23%	27%	63%	75%	29
Low	>10 to 20	14%	50%	10%	7%	0%	64%	25%	25%	16
Tenuous	>1 to 10	0%	0%	0%	14%	0%	0%	0%	0%	2
Total		7	6	10	14	60	11	8	4	120

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

Table 3e reports business impact for the 84 International linkages, of which 96% are in the High and Medium bands. Approximately 74% of the International linkages are made up of the value chain - Input, Output and Specialist Service linkages in the High and Medium bands. Only Research and Development (25%), Training (20%) and Output (2%) report any linkages in the Low business impact band at the International level.

Category		GA	IA	IN	IP	OU	RD	SS	TN	Total (n)
Business Impact										
High	>30 to 40	100%	50%	88%	88%	47%	50%	100%	60%	52
Medium	>20 to 30	0%	50%	13%	13%	51%	25%	0%	20%	29
Low	>10 to 20	0%	0%	0%	0%	2%	25%	0%	20%	3
Tenuous	>1 to 10	0%	0%	0%	0%	0%	0%	0%	0%	0
Total		1	2	16	8	45	4	3	5	84

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 115 of the 379 reported, showcasing that respondent firms engage in a 30% of their linkages across the South West. The second largest geographic scope after European (32%). However, only 10% (n=12) of which are reported as highly impactful. This is the lowest proportion of linkages reported in the High business impact band when compared with National (25%), European (61%) and International (62%) scopes.

For the cyber security sector in the South West, their main customers and suppliers are off the island of Ireland and they engage in a significant number of High and Medium valued European and International linkages. These of course are at further distances suggesting that these links are harder to form and maintain, but the market is global. European and International linkages are of most importance to the RFG.

Geographic Scope		Local	National	European	International	Total
Business Impact						
High	**>30 to 40**	10%	25%	61%	62%	152
Medium	**>20 to 30**	48%	45%	24%	35%	140
Low	**>10 to 20**	37%	30%	13%	4%	79
Tenuous	**>1 to 10**	5%	0%	2%	0%	8
Percentage		30%	16%	32%	22%	100%
Total (n)		115	60	120	84	379

Table 4: Business Impact by Geographic Scope of Linkages

Key Connectors

Figure 5 illustrates the key connectors in the South West Cyber Security sector in Ireland. 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 the South West, there are strong linkages to Research and Education institutions, Industry Associations and Government Agencies. The standout linkages for the RFG are with IDA Ireland and Cork Institute of Technology as respondents report the majority of these connections in the High and Medium bands with 92% and 77% respectively.

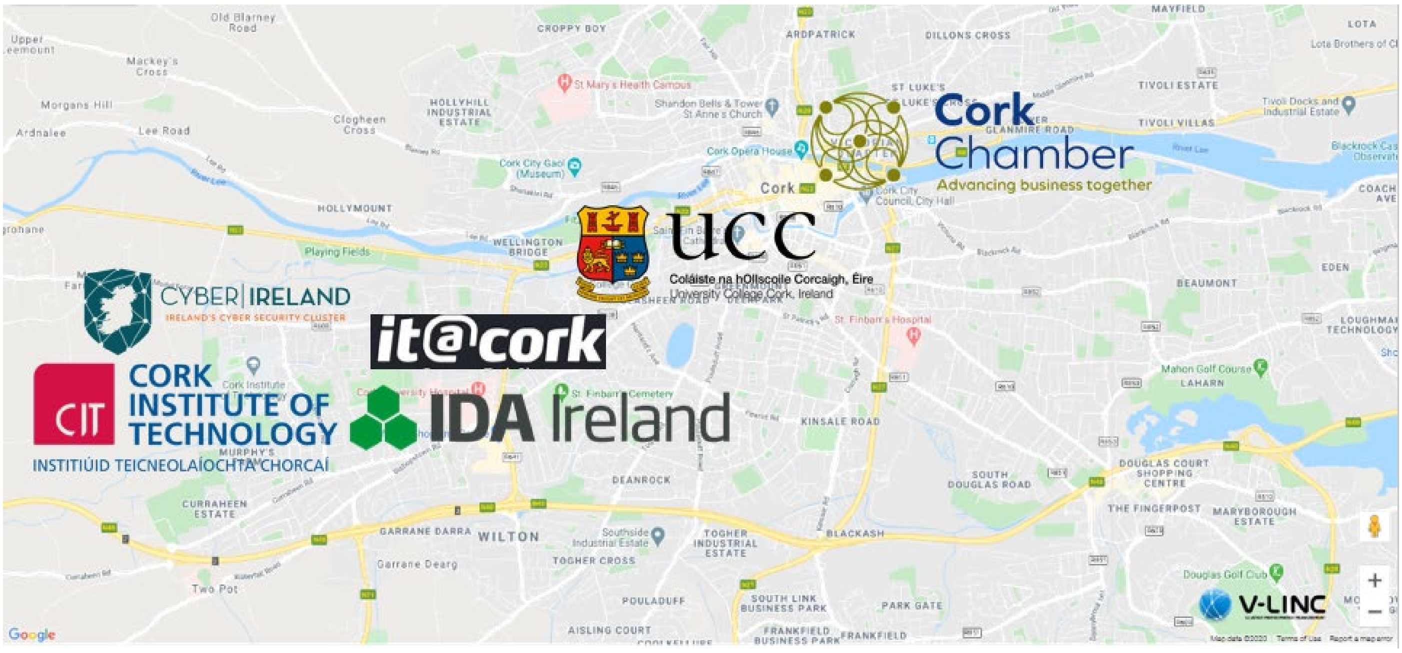

Cork Chamber
Advancing business together
UCC
Coláiste na hOllscoile Corcaigh, Éire
University College Cork, Ireland
CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER
it@cork
CORK INSTITUTE OF TECHNOLOGY
CIT
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ
IDA Ireland
V-LINC
Cork
Google

Figure 5: Key Connectors in the South West of Ireland Cyber Security Sector.

Key Connector		CIT	UCC	IDA	it@cork	Cyber Ire	Cork Chamber
High	**>30 to 40**	15%	0%	17%	25%	0%	0%
Medium	**>20 to 30**	62%	38%	75%	25%	45%	27%
Low	**>10 to 20**	15%	54%	8%	50%	55%	64%
Tenuous	**>1 to 10**	8%	8%	0%	0%	0%	9%
Total (n)		13	13	12	12	11	11
Linkage Category		6 TN, 5 RD, 1 IN, 1 SS	7 TN, 5 RD, 1 SS	11 GA, 1OU	8 IN, 4 TN	11 IA	7 IA, 4 TN

Table 5: Business Impact of Key Connectors in the South West of Ireland Cyber Security Sector.

Cork Institute of Technology and University College Cork are the most connected entities to the RFG, their linkages to the cohort of firms extend across Research, Training, Specialist Service and Input linkages. As indicated in Table 3b the Research linkages of these key connectors aren’t held in great regard by the RFG. Of the 10 research connections, 30% are in the Medium, 50% in the Low and 20% in the Tenuous band. It is evident IDA Ireland are strongly valued by the RFG and connected to the respondents. The three Industry Associations it@cork, Cyber Ireland and Cork Chamber are also heavily connected to the sector. it@cork and Cork Chamber provide skillsnet training programmes for their members, providing both an Industry Association and Training link with some respondents. As Cyber Ireland is the newest ‘Industry Association’ in existence it is positive to see them linked to all respondents as they build out their initiatives and offering for members. Other key connectors are difficult to find in the analysis, as respondent companies only identified five other organisations with whom three or more connections are made.

Policy Recommendations

Having reviewed Ireland's National Cyber Security Strategy 2019 – 2024 (Government of Ireland, 2019b) and Future Jobs 2019 (Government of Ireland, 2019a) in tandem with the results of the V-LINC analysis, the following policies aim to develop the Cyber Security sector in Ireland.

1. **Support and Strengthen collaborative R&D linkages with academia and industry, through i) a dedicated national cyber security research centre and ii) collaborative national funding programmes for R&D.**

There is a need to assist firms operating in the Cyber Security sector in Ireland, to innovate through increased R&D activity with academia/research institutions and B2B collaborations. It is evident that R&D linkages are one of the least populous linkage categories in the study (Table 3a) with just 36 linkages reported. This is surprising for a high-tech industry segment. Research linkages are a mixture of connections with academic institutions, research centres and private industry. Most R&D linkages (56%) occur at Local (Figure 6) and National levels (Table 2), however, most (67%) are deemed of Low and Tenuous importance (Table 3b and 3c). All but 2 of the 21 of these Local and National R&D linkages are with academic institutes and research centres. It seems that strong R&D connections with academia and collaborative B2B research relationships are difficult to forge in Ireland. In contrast, 4 out of 11 R&D connections at a European level and 3 out of 4 International R&D connections are B2B – significantly all of these are reported in the High and Medium business impact bands.

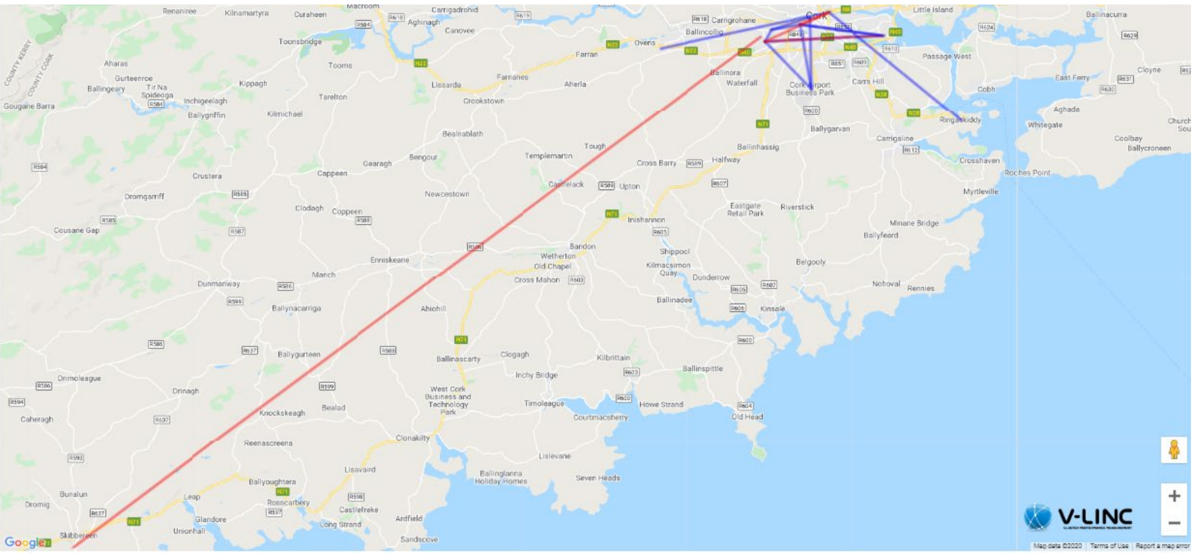


Figure 6: Local R&D linkages in the South West cyber security sector.[4]

[4] The Blue linkages are those in the Low and Tenuous bands, whilst those in Red are reported to be of High and Medium business impact.

An Industry Forum hosted in CIT in April 2017 attended by companies from the cyber security sector (SMEs and MNCs) and government agencies (IDA Ireland and Enterprise Ireland) reported low levels of collaborative cyber security R&D between industry. Furthermore, industry found it difficult to engage with academic research centres, which they felt is limiting the growth and innovation of the sector in Ireland. Cluster Initiation Workshops, organised in February 2019, gathered industry feedback to establish the strategy of the Cyber Ireland cluster. Feedback found that industry wanted: 1) a National cyber security research centre for Ireland and 2) supports to facilitate collaborative R&D between industry and academia.

It seems there is a two-pronged approach to supporting and strengthening collaborative R&D linkages with academia and B2B connections with industry:

i. Development of a dedicated national cyber security research centre

A national cyber security research centre is required to co-ordinate security-related research across the various research centres nationally, groups in SFI and academic research centres, to facilitate increased industry engagement with public R&D.

In Ireland there is significant competition between our Higher Education Institutes (HEIs), this limits co-operation as each institute wishes to compete on its own merits. Were national government to support the development of a dedicated national cyber security research centre, one way to incentivise the involvement of all HEIs is to provide postdoctoral and PhD funding for students to co-locate in the research centre, if their projects meet certain criteria and have industry involvement. HEIs would be linked to the national cyber security research centre through the supervision of their students and an academic co-working space could be made available also as part of the facility. The programme could be funded through SFI's Centres for Research Training programme which will provide funding for the training of postgraduate students in areas of identified skills needs. However, the post graduate students need to be co-located in one centre and not dispersed across many to realise the benefits. This type of initiative would facilitate companies to connect with academia at a central point and perhaps raise the business impact of the research.

ii. Developing a Collaborative R&D - B2B programme.

Developing funded co-operation projects between cyber focused firms, and with firms from other sectors, in Ireland can stimulate increased R&D linkages and innovation. In Ireland, industry is pre-disposed to the R&D supports that are provided through Enterprise Ireland and IDA Ireland, these are managed on a one to one basis – where each organisation applying receives funding to innovate with an individual HEI. Shifting the focus to work collaboratively with multiple industry (and even academic) partners may be transformative.

An example of a best practice 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 enables 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 Cyber Ireland cluster organisation, may be the conduit needed for realising more B2B market focused connections and opening further connections internationally for the sector.

The aforementioned i) and ii) measures align with the National Cyber Security Strategy 2019 – 2024 (Government of Ireland, 2019) which identifies the need to support cyber security R&D activities under measures 14 and 16.

- Measure 14 of the national strategy – “Science Foundation Ireland, along with DBEI and DCCAE, will explore the feasibility through the SFI Research Centre Programme, the Research Centre Spoke programme or other enterprise partnership programmes, to fund a significant initiative in Cyber Security Research.”
- Measure 16 of the national strategy – Enterprise Ireland will develop a cyber security programme to facilitate collaborative links between enterprise and the research community that leads to the practical application of research in business.

While both the National Cyber Security Strategy’s R&D supports for academic research and industry focused R&D are much welcomed, there is no timeline for the implementation of these measures or financial commitment in the report. A clear timeline and financial commitment are needed to ensure that industry needs are met. Cyber Ireland has a critical role to play in supporting R&D in its role as a facilitator, matchmaker and voice of industry. It seems evident that Cyber Ireland could be a central partner in the development and implementation of a national cyber security research centre or R&D programmes to support industry-academic engagement.

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. Cyber Ireland could connect academics with industry locally, and through Science Foundation Ireland (SFI) and the US-Ireland R&D Partnership connect with scientists and engineers across the three jurisdictions to increase level of collaborative R&D. Each jurisdiction supports its own research costs, via Science Foundation Ireland (SFI) in Ireland, Department for the Economy in Northern Ireland and National Science Foundation (NSF) in the US.

2) Prioritisation of Training and Education supports to Address Critical Skills Shortages in Cyber Security

As Cyber Ireland was developed in the first instance to address the critical skills shortage in cyber security, it is clear that this is a priority issue for the RFG. At present, there is 0% unemployment reported in cyber security roles worldwide, with 3.5 million unfilled jobs predicted by 2021[5], resulting in increasing global competition for talent and investment. A global study[6] from ESG and ISSA confirmed "that the cyber security skills shortage is exacerbating the number of data breaches," with the top two contributing factors to security incidents being "a lack of adequate training of non-technical employees" (31%) first and "a lack of adequate cyber security staff" (22%) second.

In Ireland, the biggest challenge to the growth and competitiveness of Ireland's cyber security sector is the immediate skills shortage, which is evident from increasing salaries, demand for cyber security graduates and international recruitment. Additionally, these shortages present a national security challenge, as companies, government departments and agencies, cannot recruit the skilled personnel to protect, respond, and mitigate against security threats and breaches. Ireland's National Cyber Security strategy spells out the urgency in addressing this critical skill shortage, and places emphasis on the need for a ready supply of talent to ensure that our data centres (which house a 30% of Europe's data), businesses and critical infrastructure, are protected. A number of initiatives aiming to address this shortage from courses/modules in HEIs, the Skillnets' Cyber Security Skills Initiative and the FIT Cyber Apprenticeship being piloted. However, these have not met the growing demand to date.

[5] https://cybersecurityventures.com/jobs/

[6] http://www.prweb.com/releases/2017/11/prweb14899778.htm

It is evident that Training is of critical importance to cyber security firms in the RFG, as the (joint) third most numerous category. Respondents reported 45 connections of which 80% are in the Republic of Ireland. It is important to assess the business impact of these links, 59% of Local (Figure 7) and 71% of National are deemed of High and Medium importance. Of further note is that none of the companies have links with ICT Skillnets, who run the Cyber Security Skills Initiative, nor with FIT, who run the Cyber Apprenticeship programme.

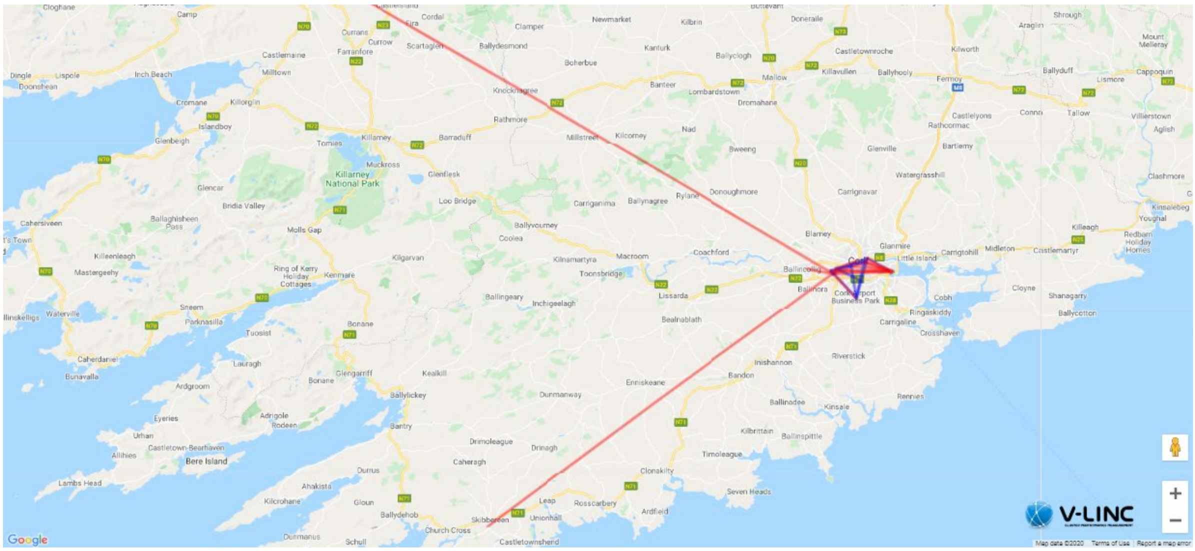


Figure 7: Local Research & Development and Training linkages in cyber security Northern Ireland.[7]

At the Industry Forum in April 2017, industry discussed the cyber security skills shortage and the need for deep, specialised and experienced talent as well as graduates that receive up-to-date education in the skills, technologies and competences of relevance to industry. This was built on at the Cyber Ireland Cluster Initiation Workshops in February 2019, where feedback via an industry survey found the top initiatives required by industry to address the skills shortage were to: (1) Outline current & future talent & skills needs of industry, (2) engage with HEIs to influence current and future course programmes to align with industry needs, and (3) promote cyber security careers and pathways to adults and children.

[7] The Blue linkages are those in the Low and Tenuous bands, whilst those in Red are reported to be of High and Medium business impact.

To address the cyber security skills shortage there is an urgent need for a co-ordinated approach from all key stakeholders across industry, academia, and government. Support and promotion for upskilling for technical staff working at the cold face of cyber security and for non-technical employees is essential. Cyber Ireland, as the national cluster organisation has a central role in understanding the needs of industry and working with the education and training providers to align courses and training to the needs of industry. Some suggested supports include:

a) Funding to conduct a national cyber security skills survey to determine where the current and future skills and skills gaps are across organisations, and in the Irish market, to understand the effects of the cyber skills shortages, the skill needs organisations are challenged to meet through training and recruitment, and identify diversity in the Cyber Security community. The UK has recently published their 'Cyber Security Skills in the UK Labour Market 2020' report[8] 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.
b) HEIs that feed into the cyber security talent pipeline need to work together and break down the silos that currently exist both within and between academic institutions. This co-ordinated group of HEIs can work with industry, through Cyber Ireland, to align courses with industry needs.
c) The Skillnets 'Training Networks Programme' supports the activities of enterprise led Learning Networks across a wide range of industry sectors and geographical regions. As Cyber Ireland is the industry representative body for Cyber Security, it could apply to run its own Skillnet, in collaboration with the existing Cybersecurity Skills Initiative.
d) To ensure the next generation of cyber security professionals, Ireland needs to support the promotion of cyber security careers, and the pathways into those careers, to young people (11 – 18 years old). There are many programmes in other leading countries for cyber security training and promotion to children, such as CyberFirst in the UK where 12,000 girls took part in the programme in 2019. There is a similar need in Ireland for a national programme to promote cyber security careers, pathways and skills to young people. This could be developed and rolled out through Science Foundation Ireland's (SFI) Smart Futures Programme, with the support of industry and other key stakeholder groups.

[8] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020

Cyber Ireland can take the lead in promoting these initiatives to all stakeholders by becoming a critical part of the solution, with their membership of over 170 organisations (140 from industry, and all of the major HEIs in the Republic). The cluster has the opportunity to co-ordinate a national training, career promotion and job availability solution for the sector in Ireland.

A careers and training portal on the Cyber Ireland site could fill a void which currently exists in Ireland. An online dashboard composed of three integral elements 1) Cyber Course Finder, 2) Cyber Careers Showcase and 3) Cyber Vacancies would be an invaluable tool and resource which could pull together the most pertinent information from Cyber Ireland members across the triple helix to support the process of addressing the skills shortages for cyber professionals in Ireland. This portal would not be a short-term fix, but a longer-term strategic play to funnel more talent into the sector. A resource which could be used by secondary school students to see the types of careers on offer, life-long learning for employees and students whom wish to study, upskill, or transfer from another discipline, and for industry to promote the vacant roles they have on offer.

3. Connect the Multinational and Indigenous players on the Island of Ireland.

As mentioned previously, the low numbers of Industry Peer linkages, the least numerous of the categories overall (Table 1 and 3b), indicate difficulties the RFG have in building trust-based collaborations with competitors, something Porter (1990, 1998b) highlights as essential in any cluster. This is further exasperated by the fact that the RFG report 88% of Industry Peer linkages at European and International levels, which shows less than a handful of connections across Ireland in this category. From a European and International perspective, these links are highly valued with 78% and 100% of these connections in the High and Medium impact bands. The question is why such links are not occurring in Ireland?

One particular programme Cyber Ireland could run as part of their services for industry could be 'Deal Broker' a programme which was originally run as part of the EU funded, Framework Programme 7, Be Wiser project - a collaboration between CIT and it@cork. The aim of the programme is to highlight a selection of Irish SMEs to large multinationals, and other indigenous firms in the region, to showcase the vibrant SME community that exists and foster relations between both parties. Large companies get the opportunity to hear the product offering from the SMEs in a unique environment and speak to them on a one-to-one basis to explore, and hopefully foster engagement. It is not a "pitching for investment" event, but rather an opportunity to meet and hear some new technologies that are being developed. Participants may wish to partner to develop collaborative business, research, mentoring, or feedback in the future.

After a ‘tour de table’ to introduce all participants in the room, so that organisations have an idea of who they would be pitching to, the indigenous SMEs are given 10 minutes to present to the MNCs and large indigenous firms in attendance. There is also an opportunity for MNCs and large firms to pitch their current challenges to see if the SMEs could meet their needs.

Perhaps further opportunity could be leveraged through the InterTradeIreland Synergy programme to extend this action in to a ‘Cyber Island Deal Broker’ by bringing together the right people and companies to find a common pathway to solve shared problems in both Ireland and Northern Ireland and connect the sector collaboratively.

Closing Remarks

This paper has described and applied the V-LINC methodology for identifying and analysing the linkages that cyber security firms in the South West of Ireland engage in. For Cyber Ireland to support and formalise the success of the sector through growth and expansion in the global marketplace, additional effort is required to address the problems and opportunities identified.

The analysis shows evidence of strong European and International connections developed from the South West, however if a fully functioning cluster is to develop, which will have further impacts on economic growth, there is a need for increased competition and co-opetition. Research and Development connections will need to be forged more strongly both with academia and at a B2B level, whilst much work is required in addressing the Skills requirements to ensure a flow of talent exists to drive and nurture the cyber sector.

CIT secured two years funding from IDA Ireland to facilitate the establishment of a cluster organisation to represent the cyber security sector and address key challenges identified by industry. Cyber Ireland launched in May 2019 and is still in the initiation phase of its development. In this short time, it has already gained the buy-in of industry, academia, and government as can be seen from its 170 members. The NCSC has acknowledged the importance of Cyber Ireland’s role and will support the organisation; Measure 15 of the national strategy states: “Government will continue to support and fully engage with the IDA funded Cyber Ireland Programme and explore new mechanisms to support Industry/Academia/ Government cyber security collaboration” (Government of Ireland, 2019). Furthermore, Cyber Ireland has won funding under the Regional Technology Cluster Fund to support the indigenous section of the cluster. This funding, along with other revenue streams from industry will sustain the cluster activities going forward.

Table 5 and Figure 5 show that Cyber Ireland is connected to each of the respondents who participated in this analysis study. With its remit to provide a collective voice for the cyber security cluster, Cyber Ireland is the conduit connecting participants with others across cyber security in South West, and nationwide (Figure 6). The data in this report suggest that respondent firms see the potential for real value in connections with Cyber Ireland (Table 5) even though the cluster is at a very early stage in its development.

While Cyber Ireland has been successful to date in its initiation and has the backing of key government agencies; one difficulty which exists is that there is no national cluster policy in Ireland that outlines the role of cluster organisations in supporting economic growth and innovation. There is also no dedicated national funding stream from government for cluster organisations to support their activities. Therefore, the role of cluster organisations, their KPIs and funding supports are unclear, and this puts into doubt the long-term sustainability of cluster initiatives in Ireland.

Strategies targeting clusters of regional specialisations can help address the fragmentation and unfocused investment that sometimes undermines the emergence of new marketable products and technologies. ICN (2014) suggests that a cluster organisation can have a significant influence on strengthening collaboration in a cluster, through the implementation of effective innovation policy. Regions across Europe that have been successful in supporting economic growth, competitiveness, and innovation through clusters have a national policy or framework of dedicated funding and supports e.g. Catalonia (ACCIO), Flanders (Spearhead Clusters - Vlaio), Paris (Pôle de Compétitivité) and Piedmont (Innovation Poles) are noteworthy.

Future research may analyse other regional pockets of the Cyber Ireland cluster – potentially in Limerick / Galway and Dublin / East Coast to compare and contrast their linkages with that of Cyber Ireland members in the South West of the country. Additionally, the long-term funding model for the Cyber Ireland cluster, will need to be evaluated. In European regions, public financing is available to fully support a cluster organisation's operations in its first 2-3 years (Hobbs, 2010; CEBR, 2014; ECO, 2013; Byrne, 2016). Cyber Ireland as a 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, especially in the context of the lack of a National Cluster policy. This type of funding has allowed regions, like Catalonia (ACCIO), Flanders (Spearhead Clusters - Vlaio), Paris (Pôle de Compétitivité) and Piedmont (Innovation Poles), source funding for cluster management and research and innovation activities from European Aid for innovation clusters under the General Block Exemption Regulation .

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.
- DESI (2019), 'European Commission Digital Economy and Society Index 2019,' Available Online @ https://ec.europa.eu/digital-single-market/en/desi.
- 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.
- Eurostat, (2016), 'Tertiary education graduates: main subject areas,' European Union. Available online @ https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20190125-1.
- Government of Ireland (2019a), 'Future Jobs Ireland 2019: Preparing Now for Tomorrow's Economy,' March, Available Online @ https://dbei.gov.ie/en/Publications/Publication-files/Future-Jobs-Ireland-2019.pdf.
- Government of Ireland (2019b), 'Ireland's National Cyber Security Strategy 2019 – 2024,' December by NCSC, Available online @ https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf.
- 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.
- IDA Ireland (2018) 'Cork's cyber security credentials to the fore,' Accessed on 10th February 2020, Available online @ https://www.idaireland.com/newsroom/blog/may-2018/cork%E2%80%99s-cybersecurity-credentials-to-the-fore.
- IDA Ireland (2019) 'Why Ireland for Cyber Security,' Accessed on 10th September 2019, Available online @ https://www.idaireland.com/newsroom/publications/why-ireland-for-cyber-security.
- Irish Tech News (2019), 'The Time is Now to Make Ireland A Cyber Security Centre Of Excellence,' by Ronan Leonard, February 27, 2019, Available online @ https://irishtechnews.ie/the-time-is-now-to-make-ireland-a-cyber-security-centre-of-excellence/.
- 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 @ http://www.tmg.at/1003_ENG_HTML.php