# MAPPING THE CYBER ISLAND

V-LINC analysis of NI Cyber and Cyber Ireland clusters to understand the functioning of the ecosystem for cyber security firms on the Island of Ireland


**Prepared by:**
Project Partner: V-LINC Cork Institute of Technology

**Funded by:**
InterTradeIreland

CIT CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

InterTradeIreland

**Publication Date:** 01/09/2020



Written and Compiled by Dr John Hobbs, Dr Eoin Byrne, Dr Cliodhna Sargent and Tabona Kuli, CIT.

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

Cross-border trade in goods and services on the island of Ireland has grown exponentially over the past twenty years[1]. Whilst, clarity on the impact on trading relationships is yet to emerge from Brexit negotiations, InterTradeIreland is keen to ensure that cross-border trade continues to grow. Over the past two decades cross-border trade has proven to be robust recovering strongly from shocks such as the banking crisis, which have made local businesses in both the Republic and Northern Ireland more resilient.

Like the rest of the developed world, technology has come to play a central role in supporting and facilitating economic and social life. The island of Ireland has also gained very significantly in economic terms from development of a global data ecosystem; our geographic position, and strong links to the US have ensured that we have become host to a significant amount of data and economic activity. Cyber security is becoming the core of this activity.

Mapping the Cyber Island seeks to shed light on the North/South linkages and connections of the cyber security industry, and the potential supports required to buttress the sector as it develops towards one of importance in the Republic and Northern Ireland. To add some perspective, IDA Ireland (2018) reports that Ireland's cyber security sector employs approximately 6,500, whilst the cyber security sector in Northern Ireland employs almost 1,700 people 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).

Cyber Security is often described as the means of ensuring the confidentiality, integrity, authenticity and availability of networks, devices and data. However, as network and information systems become more embedded and complex, securing these becomes simultaneously more important and difficult. While these responses have evolved quickly in an attempt to keep pace with technological and market developments, this process is made vastly more challenging by the extremely dynamic nature of developments, both in terms of technology and in terms of the global strategic environment (Government of Ireland, 2019b).

[1] https://intertradeireland.com/insights/publications/a-simple-guide-to-cross-border-business-latest-edition/

To gain perspectives on the supports required to link cyber security firms in the Republic and Northern Ireland, the authors worked with Cyber Ireland [2] and NI Cyber, two cluster organisations which bring together Industry, Academia and Government to represent the needs of the Cyber Security Ecosystem. These clusters aim to enhance the Innovation, Growth and Competitiveness of the firms and organisations that make up their respective clusters.

A V-LINC analysis was applied to understand the linkages and connections which cyber security firms in both the Republic and Northern Ireland engage in from local, crossborder and international perspectives. V-LINC provides a framework within which to interview a sample of firms in a sector, to understand the business linkages which these firms operate across their value chain, regulatory, RD&I and training functions. V-LINC uses specially designed software to visualise this information to provide a geographic footprint of the firms' connections. The business impact of firms' linkages is also measured. When respondent firms' data are combined, visualised and analysed an understanding of the various linkages that clustered firms engage in, allows targeted policy recommendations to be developed to solidify strengths and address cluster weaknesses.

The Mapping the Cyber Island analysis provides a thorough account of the types, geographic scope and impact of linkages which a sample of 11 member firms from Cyber Ireland and 10 from NI Cyber engage in. One of the benefits of the V-LINC analysis is its ability to visualise the connections between various actors in a cluster ecosystem. Examples of the connections respondents have, are showcased in Figures 1 and 2 which visualise the value chain (customer and supplier) linkages reported by firms from Cyber Ireland (Blue) and NI Cyber (Red). These connections are shown locally and nationally in Figure 1, and across Europe and internationally in Figure 2. A highway of linkages between the South West and Dublin exists (Cyber Ireland respondents), whilst similarly numerous linkages between Belfast and London are apparent (NI Cyber respondents). Cyber Ireland respondents are heavily connected across Europe, whilst further afield both Cyber Ireland and NI Cyber firms have numerous connections with North America and Asia.

[2] Cyber Ireland is a national cluster organisation which brings together Industry, Academia and Government to represent the needs of the Cyber Security Ecosystem across the Republic of Ireland. Its aim is to enhance the Innovation, Growth and Competitiveness of the companies and organisations which are part of the cluster. In this report a sample of member firms from the South West of Ireland were interviewed to gain an understanding of this specialisation of Cyber activity in Ireland.

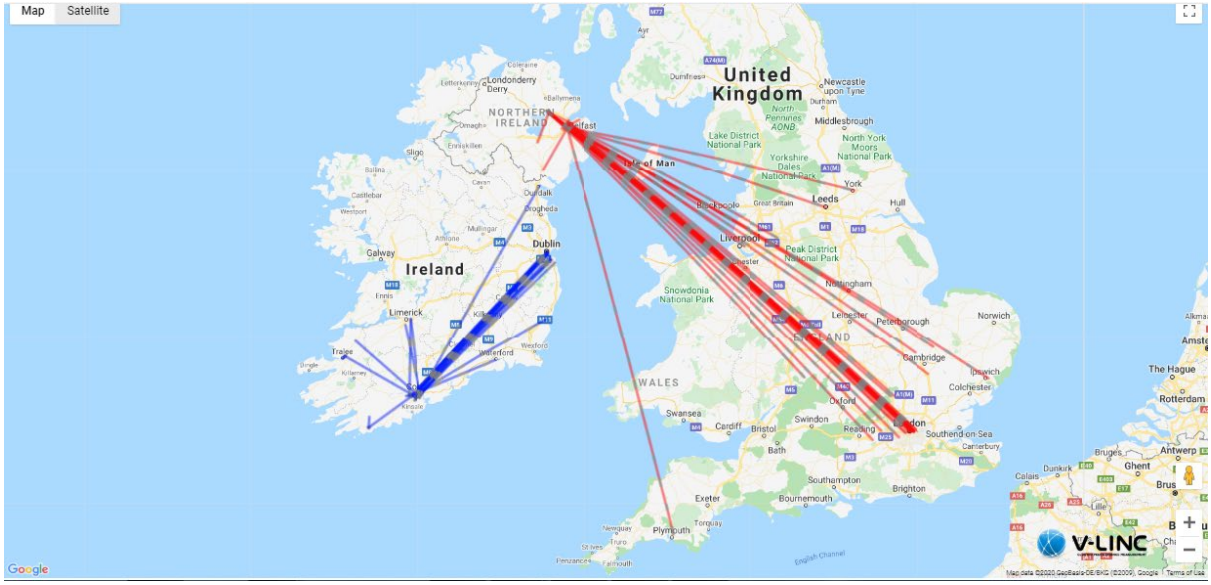


**Figure 1: Local and National value chain (customer and supplier) linkages reported by the member firms of Cyber Ireland (Blue) across Ireland and NI Cyber (Red) across the UK.**


**Figure 2: European and International value chain (customer and supplier) linkages reported by the member firms of Cyber Ireland (Blue) across Ireland and NI Cyber (Red).**

If we focus on customers, or output linkages alone, Figures 1 & 2 above show the importance of global markets for cyber security firms. Cyber Ireland respondents (Blue) report that 95% of Output linkages are reported outside Ireland, with 54% destined for the European marketplace and 41% for International markets. Whilst NI Cyber firms report that 86% of output linkages are outside Northern Ireland, of which 23% is destined for the UK, a further 17% for the European marketplace and 46% with international customers.

When analysing the V-LINC results from Cyber Ireland and having reviewed Ireland's National Cyber Security Strategy 2019 – 2024 (Government of Ireland, 2019b) and Future Jobs 2019 (Government of Ireland, 2019a) the following policies are proposed to support the development of 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.
2. Prioritisation of Training and Education supports to address critical skills shortages in cyber security.
3. Connect Multinational and Indigenous players across the Island of Ireland.

Further context and support for these recommendations are outlined in the section V-LINC Highlights – Cyber Ireland (South West), as part of this report.

When analysing the V-LINC results from NI Cyber and reviewing Cyber Security: A Strategic Framework for Action 2017-2021 and UK National Cyber Security Strategy 2016-2020 the following policies are proposed 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.
2. Prioritising facilitation of B2B and academic research and development linkages.
3. Facilitate and Focus on the Internationalisation of Micro and SME Cyber Firms.

The context and support for these recommendations are outlined in the section V-LINC Highlights – NI Cyber (Northern Ireland), as part of this report.

To connect these recommendations from an all island perspective, there is opportunity through leveraging the InterTradeIreland Synergy[3] programme to jumpstart the connection of both collaborative B2B trade and RD&I between industry and academia by identifying a common pathway to solve shared problems in both Ireland and Northern Ireland.

[3] Synergy is InterTradeIreland's cross border cluster initiatives that aims to increase the growth and competitiveness, by supporting synergistic cross-border connections between networks, partnerships, sectors and clusters on the island of Ireland. https://intertradeireland.com/corporate-information/our-strategy/

Finally, regarding current trade levels and appetite for cross-border collaboration the V-LINC interviews also sought to ascertain current levels of trade and interest in collaborative opportunities to further connect the sector in Ireland and Northern Ireland. Table 2, showcases that half of the respondents in both jurisdictions are trading with counterparts across the border, albeit at low levels of overall turnover in the majority of instances.

In Table 3, it was clear that respondents from Ireland (91%), and Northern Ireland (70%) were interested in participating/attending in cross border conferences. This was followed by networking with respondents from Ireland (73%), and Northern Ireland (60%) interested in participating – with Business Collaboration / Pitching / Elevator Pitches mentioned by respondents.

Respondents from Ireland (73%) were interested in visiting Belfast to look at the resources such as, CSIT and the Digital Catapult, whilst only 10% of Northern Ireland respondents were interested in visiting Ireland. It cannot be underestimated the focal point such R&D and enterprise support incubators can provide for a sector in a region, and it is obvious that the respondents from the Republic of Ireland are aware of the world class standing of both CSIT and the Digital Catapult. It is also understandable that there is no equivalent in the Republic of Ireland focused on cyber security that has built such a reputation and this effectively explains the lack of interest in study visits from Northern Ireland respondents as there is no focal point for the sector in Ireland.

Mapping the Cyber Island sets out a pathway upon which Cyber Ireland and NI Cyber can embrace the present challenges faced by the cyber security sector, their members and take advantage of the enterprise and job creation opportunities flowing from these global technological developments. This report develops a series of recommendations designed to address some of the complex challenges currently facing Cuber ireland and NI Cyber members associated with sustaining and growing the number of people employed in this sector.

## INTRODUCTION

InterTradeIreland have funded a V-LINC analysis of a sample of Cyber Security firms connected to Cyber Ireland and NI Cyber to understand the ecosystem in which firms at one end of the island (South West) operate in when compared to the other (Northern Ireland).

The V-LINC methodology identifies, records and analyses the linkages that firms in sectors and clusters engage in. V-LINC was developed in Cork Institute of Technology to enrich academic literature on clusters. V-LINC visualises information on the geographic footprint of cluster ecosystems, whilst measuring the perceived 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 address cluster weaknesses.

The benefit of the Mapping the Cyber Island report is twofold:

• The analysis provides a thorough account of the types, geographic scope and impact of linkages which a sample of 11 member firms from Cyber Ireland and 10 from NI Cyber. This provides an in-depth understanding of the value chains these firms engage in and a gap analysis of their current needs. It supports the respective Cluster Managers in each jurisdiction to understand their members and represent them more effectively.

• Collectively the analysis provides a cluster mapping and visualisation of the members of Cyber Ireland and NI Cyber and their Irish, European and International connections, providing an overview of the strengths and potential gaps with each cluster ecosystem. This data will highlight current and new areas for collaboration from product, service, research, innovation and / or training perspectives.

As the cyber security sector on the island of Ireland develops and expands it is important that industry players, business support organisations and policy makers understand how the cyber security ecosystem operates along with its external relationships. So that collaboratively, they can deliver growth and employment through supportive policies.

It is an exciting time for clustering on the Island of Ireland as organisations like the Department of Business, Enterprise and Innovation in Ireland, Department for the Economy in Northern Ireland, IDA Ireland, InterTradeIreland, Invest NI and Enterprise Ireland are beginning to promote and support clustering as an economic development tool through initiatives like the Collaborative Growth Programme, Regional Economic Development Fund and Regional Technology Cluster Fund. Whilst these cluster programme support initiatives are positive, there is also a need for a clear framework of what constitutes a cluster and what is their role in supporting economic development. In the absence of clarity and formalised national ROI and UK clustering policies, standalone supports for clustering could result in a haphazard approach and detrimentally effect the long-term supports for, and benefits of, clustering on the island of Ireland.

This report begins by outlining the definitions for a cluster, cluster organisation, and cluster initiatives. Next it describes why cluster mapping and visualisation is an important tool in understanding an ecosystem – and showcases the V-LINC methodology which is applied in this research. A short introduction to cyber security is provided, after which a synopsis of the V-LINC analysis reports for Cyber Ireland and NI Cyber, including key recommendations, are proposed.

The final section showcases the 'Map' of the Cyber Island, which identifies the key cyber security players in the South-West and North of the island. The report concludes by presenting the areas where firms interviewed as part of the study believe there are opportunities for collaboration between the both clusters.

## CLUSTERS AND CLUSTER ORGANISATIONS

Clusters are characterised by their industrial specialisation and an above average concentration of employees within that industry, for example: Italy's sports car cluster, Modena; chocolate in Switzerland or filmmaking in Hollywood, USA.

Some key definitions are:

- A cluster "is a geographical proximate group of interconnected companies and associated institutions in a particular field, linked by commonalities and externalities" (Porter, 1990).
- A 'cluster organisation' on the other hand is a formal institution that is established to facilitate increased interaction and cooperation between participants in the cluster, often with public development agencies as important contributors.
- A 'cluster project/initiative' is a targeted effort over a limited period to strengthen and accelerate development of the cluster. This is achieved through a wide range of strategic activities aimed at strengthening a cluster's and participants' competitive positions.

Another hallmark of clusters is that due to their overlapping industries and geographic proximity, there are significant knowledge spill-overs between firms and institutions. These can occur formally at seminars organised by a cluster manager, or casually when two professionals meet by chance at a cafe. These spontaneous connections, catalysed by overlapping industries and proximity, characterise a cluster.

There are two types of clusters: local clusters are found everywhere, while traded clusters are found only in specific regions with factors conducive to the trade of goods and services across jurisdictional boundaries, such as between provinces. Local clusters primarily serve the local market, such as retailing centres or utility companies. Traded clusters have an international client base and include well-known exporting industries such as aerospace, automotive production, biopharmaceuticals and cyber security.

Traded clusters also include non-exporting firms such as educational institutions and hospitality/tourism, whose revenue is generated by foreigners paying for goods and services. Since traded clusters are able to access a larger customer base by exporting, they are, on average, more innovative and profitable than local clusters.

## WHY IS CLUSTER MAPPING AND VISUALISATION IMPORTANT?

Visualisation of cluster ecosystems offers insight into how a cluster functions, who the key actors are and how they are connected, offering a picture of multi-stakeholder network and the variety of different relationships featured across different actors. Whereas multi-stakeholder approaches focus on focal organizations (Freeman, 1999), cluster analysis encompasses many organisations, a variety of relationships and a geographical scope.

Clusters are dependent on external factors. It is not uncommon to find highly localized clusters with stronger foreign ties in, for example, research collaborations than with domestic research institutions. For this reason, a network analysis is useful for gauging a cluster's various strengths and weaknesses.

To visualise a cluster ecosystem, key linkages must be identified and measured utilising:

- a method to collect firm linkage data;
- analysis to produce targeted policy initiatives.

V-LINC methodology (Byrne, 2016) adapts the *Four i Linkage Scale* (Hobbs, 2010) and incorporates network theory to support data collection applicable across clusters and regions. It places firm linkages at the core of the analysis and builds on social network analysis maps (although V-LINC does not employ techniques of social network analysis). To generate a visualisation of the linkages engaged in by firms in a cluster and plot the linkages geographically a software tool was developed.

V-LINC facilitates policy development at local and national levels through the aggregation of data from a sample of firms. Confidentiality of firms' linkages is maintained throughout the entire process. The result of this type of analysis is two key pieces of information which 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 organizations 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 (rather than relying on outside talent.)

## MEASURING LINKAGES

In measuring linkages, categories of linkage must be identified. In a cluster, co-located firms are connected in some way which results in superior performance, relative to spatially dispersed non-cluster firms (Porter, 2000b). Significantly, geographic proximity does not guarantee the benefits of agglomerations and clusters (Bathelt et al., 2004; Boschma, 2005; Tallman and Phene, 2007). It is the social networks that are generated across cluster actors that explain at least part of their performance, and innovation (Owen-Smith and Powell, 2004; Singh, 2005; Whittington et al., 2009). A network "consists of a set of actors or nodes along with a set of ties of a specified type that link them," (Borgatti and Halgin, 2011, p. 2) which, from the perspective of economic geography, implies *something* in the nature of the connections between firms (and cluster actors) influence the local economy.

Connections between actors within and external to a cluster, serve various purposes. Porter (1998a) delineates these linkages as vertical relationships (between buyers/customers in the value chain) and horizontal relationships (across an industry for firms with similar technologies or customers). Historically, measuring input and output links has provided the backbone to research studies on concentrations of firms (Porter, 1990, 1998b; Sölvell, 2008; Sölvell et al., 2009). Porter's (1998a, p. 78) theory further highlights the importance of linkages with other "governmental and other institutions, such as universities, standard-setting agencies, think tanks, training providers, and trade associations, who provide specialised training, education, information, research and technical support." The latter support collaboration and serve a productivity-enhancing purpose for the cluster.

Hence, the first step in measuring linkages demands defining the category of linkage. V-LINC builds on value chain transactional approaches, and records linkages across eight different categories derived from cluster theory on linkages (Marshall, 1890; Porter, 1998a and Leydesdorff, 2012). The eight linkage categories are presented in Table 1.

1. **Government Agency linkages (GA):** comprise all forms of linkages to government departments and agencies including state support for enterprise; e.g. regional authorities and local government agencies.
2. **Industry Association linkages (IA):** includes all memberships and relationships with organisations for collaboration; e.g. industry association groups, chambers of commerce, cluster organisations.
3. **Industry Peer linkages (IP):** defined as formal and informal relationships with companies in similar or *related* industries, e.g. related via shared technologies or targeting complementary markets.
4. **Input linkages (IN):** links with suppliers of raw materials, goods and services with a critical impact on the end product or service of the surveyed firm.
5. **Output linkages (OU):** relate to customers of a surveyed firm and channel sellers from both a goods and services perspective. Outputs may be with individual customers or assigned to customer segments and regions.
6. **Research and Development linkages (RD):** include research and development relationships between companies and also with academic and research institutes.
7. **Specialist Service linkages (SS):** relationships with vendors who supply other essential services to a surveyed firm (outside of inputs) where expertise or capacity unavailable in-house e.g. services specific to an industry, distribution, IT, consultancy, marketing, financial and legal services.
8. **Training linkages (TN):** including third parties providing specific training /learning for employees, e.g. relationships with academic institutes for modules addressing skills needs now/for future.

**Table 1: V-LINC: Linkage Categories**

V-LINC provides a flexible framework to investigate cluster boundaries, or local geographic scope. Clusters are not necessarily limited to administrative or geographical boundaries, but have a geographical centre (Christensen et al., 2012). Cluster boundaries may be defined by administrative regions or distances/times employees are willing to travel (Rosenfeld, 2002); a standard radius of two hours driving time is used by Lublinski (2002).

The 'local' boundary is defined using three questions:

1. In what geographic area are firms participating in the cluster resident?
2. What administrative region(s) does the cluster encompass e.g. a NUTS level 1, 2 or 3 regions?
3. Is regular face-to-face contact between the actors in the cluster possible (e.g. are the firms within 150km or two hours driving time of the centre)?

Linkages outside the cluster locality, but within the country, are regarded as external to the cluster, and are defined as 'national'; linkages with firms outside national boundaries but within Europe are denoted 'European'; remaining linkages are 'international' (for our context, outside of Europe).

**Business Importance of Linkages:** V-LINC adopts a *Four i Linkage Scale* (Hobbs, 2010) relating each of linkage to four dimensions of Intensity, Importance, Involvement and Investment. The opinions of company personnel on the eight linkages and four dimensions and are collected through a series of Likert scale responses from structured interviews. The Likert scale used converts qualitative judgements into numerical data to be compared and subjected to further analysis. . Each dimension is scored from 1 – 10 by interviewees with the summation of results for the four dimensions providing the business importance score for each linkage out of a maximum score of 40. Scores for each linkage fall into one of four bands for ease of interpretation: "High" Band (>30 to 40), "Medium" Band (>20 to 30), "Low" Band (>10 to 20) and "Tenuous" Band (1 to 10).

Taking into account *both* the nature and extent of linkages allows for in-depth understanding of linkages and network features of a cluster. Such information allows researchers to determine which types of linkages are most and least important to firms, at what geographic scope the most important linkages occur and how important local/other cluster linkages are. Furthermore, it is possible to identify which are the most significant organisations within the cluster to specific firms. This data can also act as an evaluation technique for organisations involved in supporting business development e.g. industry associations and government agencies.

The V-LINC method to collect firm linkage data takes consideration of the Tailored Design Method - TDM (Dillman et al., 2014), which asserts that survey response can be explained in terms of the theory of social exchange. TDM provides a comprehensive set of theoretically based and empirically tested guidelines for survey design, questionnaire construction and questionnaire implementation (Fahy, 2001). In the research design, the following aspects are considered from TDM: 1) How can the perceived rewards for responding be increased? 2) How can the perceived costs for responding be reduced? 3) How can trust be established so that people believe the rewards will outweigh the costs of responding?

## PHASES IN APPLICATION OF V-LINC

**Regional Review:** Before V-LINC is applied to a cluster, a review of the regional context is conducted to establish its important characteristics including geographic and economic indicators (location features, GDP, employment and enterprise statistics). Relevant economic and industry policies are reviewed to provide additional context for later analysis. Additionally, descriptive information on the local cluster and/or industry organisation is collated. Backgrounding the regional context provides quantitative and qualitative perspectives prior to interviews with cluster members.

**Cluster Definition:** Defining the cluster is the next phase and involves delineating which industry sectors are incorporated within the cluster definition and its geographic boundaries (i.e. what constitutes 'Local'). These are defined in collaboration with a local partner organisation (trade association, chamber of commerce or cluster organisation). Firms in the local region constituting the population of the cluster are then identified and from the target population a sample of firms are selected to interview (due to the resource-intensity of face-to-face interviews). Sampling of firms from the cluster population is conducted in collaboration with the local partner organisation to gather a non-probabilistic sample. While the approach does not allow for generalising about the population, it permits study of select firms, which as active cluster members are open to participating in such analysis. The approach has the advantage of enabling policy initiatives to be developed – with increased likelihood of participation and potential to benefit relative to non-cluster members.

**Invitation to Participate:** The selected sample of firms is invited to participate. An invitation to potential participant firms includes: the aims of the study, short description of the type of information requested, time commitment involved, and why they should participate.

**Data Collection & Facilitation:** Interviews are arranged typically at the firm's premises (or the local partner organisation's office). Personnel with potential knowledge of the linkages in the eight V-LINC linkage categories are selected for interview.

**Data Validation, Upload and Visualisation:** Upon completion of interviews, data is checked, validated and uploaded to the software. To check and validate the data, any errors made while filling out the data collection form need to be identified and then rectified. The region and street address of the linkages are cross referenced using Google Maps and input into the Excel worksheets. V-LINC software uses Google Maps and a built in "find" function, which checks if V-LINC can verify the correct address for each linkage on Google Maps. This permits the researcher to identify when the recorded address gives an incorrect location, thus ensuring accurate mapping of firms' linkages. The V-LINC software converts the data into visual maps and tabular form to generate a report for each firm. Linkage data across sampled firms are collated to generate a cluster report. From the V-LINC data, *Key Connectors* for the cluster are identified through the number of linkages they have with respondent firms, and subsequently the importance of those linkages to respondents is reported. The perceived significance of key connectors allows for evaluation of their role and importance to the firms - which is an important parameter in gauging how crucial the key connectors are.

**Data Interpretation and V-LINC Reports:** The final phase in the V-LINC process consists of analysis of data and visualisation within the regional context. Policy initiatives are developed from the results to address weaknesses and leverage strengths of the cluster. Policy initiatives are developed with the expert judgement of the local partner organisation, improving the validity of the initiatives and their fit with the region and cluster specificities, to maximise their value, practicality and achievability for cluster members. A standardised firm report is provided to each participant firm and cluster report to the key stakeholders.

The next section looks at the cyber security sector, its role in our lives, the European market and introduces the context in the South West of the Republic of Ireland and Northern Ireland.

## CYBER SECURITY

The European Union Agency for Network and Information Security (ENISA) defines cyber security as "all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats" (ENISA, 2017). Cyber security has over the past decade become a priority for governments, companies and citizens. This focus on cyber security grows with each cyberattack or data leak, and garners increasing media coverage. With the digital transformation of all sectors of society, cyber security has become a crucial issue with growing needs for smart and user-friendly solutions designed to secure digital systems at large.

Confronted by the necessity to improve EU cyber security in order to ensure the safety and resilience of the economy and society, EU institutions and Member States are strengthening the regulatory framework. Measures have been taken to tackle cyber challenges, including the establishment/reinforcement of national/European cyber security strategies[4].

The first EU-wide Cybersecurity legislative act was the NIS Directive (Network and Information Security directive, part of the EU Cyber Security Strategy), adopted in 2016. The NIS Directive sets mandatory minimums for cyber security capabilities in Member States for the protection of critical sectors. Seven categories of OES (Operators of Essential Services) are identified in the Directive: Financial market infrastructures, Banking, Transport, Drinking water supply and distribution, Healthcare, Energy and Digital infrastructure. In June 2019 the EU Cyber Security Act sets the legal framework of the Digital Single Market, updating the mandate of the EU Agency for Network and Information Security (ENISA) and enabling the creation of an EU cyber security certification scheme for ICT products, services and processes.

The objective of the Digital Single Market is to eliminate unnecessary regulatory barriers. Such measures could, according to the EC, contribute €415 billion annually to the bloc's growth, boosting employment, competition, investment and innovation. In the long run, the Digital Single Market initiative will likely generate significant market opportunities, with the European cyber security market expected to grow to over €31.5 billion by the end of 2019.

[4] "Cybersecurity in the European Digital Single Market", High Level Group of Scientific Advisors, Scientific Opinion n°2, Scientific Advice Mechanism (SAM), European Commission, 2017, URL: https://ec.europa.eu/research/sam/pdf/sam_Cybersecurity_report.pdf

The dominant position of US IT and cyber security firms could pose difficulties for the emergence and scale-up of European actors. Europe boasts an expanding number of niche companies offering cutting-edge technologies, and quality Research and Development. This, combined with recent regulations to strengthen cyber security capacities across the EU, could lead to a window of opportunity for European cyber security providers. Proposals for a "European Future Fund" could see €100 billion go to high-tech European companies, enabling them to compete with larger US or Chinese players such as Google, Apple and Alibaba.

IDA Ireland (2018) believe 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) in cyber security companies or others with specific security operations (Ireland's cyber security sector employs approximately 6,500). Trend Micro was the first security company to set up in Cork over 15 years ago, now employ over 250 people. McAfee employs more than 350 people at its Cork site, which includes a security operation centre, engineering and Advanced Threat Research team. Others in the region include Cylance, Malwarebytes, eSentire, AT&T Security, Sophos, TransUnion, and Keeper Security. Since 2013, pure-play firms have announced 850 jobs in the South West.

Cyber security research in Ireland is dispersed across a number of academic institutes and national research centres. For example across the academic institutes, there is: UCD Centre for Cyber security and Cybercrime 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 industry to engage with academia and a lack of a co-ordinated national approach to cyber research.

An analysis of the UK's cyber security industry prepared by Donaldson et al. (2020) Cyber Security Sectoral Analysis 2020, showcases that the industry at the end of 2019 was worth an estimated £8.3 billion, with total revenues in the sector up 46 per cent from £5.7 billion in 2017. The number of active cyber security firms in the UK is over 1,200 at year-end 2019, with approximately 43,000 full time employees working in the cyber security sector.

The cyber security sector in Northern Ireland 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).

Critical academic/research supports in Northern Ireland have been central to the development of cyber security. Centre for Secure Information Technologies (CSIT), Queen's University Belfast, which is the UK's Innovation and Knowledge Centre. To work with industry, CSIT provides academic and engineering support for the London Office for Rapid Cybersecurity Advancement (LORCA), to help start-ups to scale at pace, to access and grow into new markets, secure further investment, and recruit and retain 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, based in the Titanic Quarter. The 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. Working closely with a network of organisations from all over the region, Digital Catapult Northern Ireland shares the mission of supporting companies based in the region to scale and grow by realising and adopting innovative digital technologies.

## HOW WILL LEAVING THE EU IMPACT ON THE UK'S CYBER SECURITY?


With the UK having a large proportion of the European cyber security market, it is prudent to mention some of the elements which may be impacted by Brexit. As the transition period is in place until December 31st, 2020 with the possibility of it being extended upon agreement from both sides. During this time most agreements currently in place will remain.

Although the UK has ceased its membership of the EU's political institutions, including the European Parliament and EC, it will have to follow EU rules and regulations. The Information Commissioners Office (ICO) says it will be 'business as usual' for data protection and GDPR. What is less certain is what will happen at the end of the transition period, especially if there isn't a trade deal in place. Unless the UK is granted a data adequacy agreement in relation to GDPR then transfer rules will apply to any data moving South to North. In addition, while the UK has currently taken on a similar set of rules to GDPR, there is potential for these to diverge over time, creating uncertainties even if adequacy is granted. Organisations will need to consider how to prepare.

If Brexit brings about also the end of free physical movement across UK borders, the cyber security talent pool – with its skilled EU nationals – may well be depleted further. It is predicted that Brexit will discourage many skilled jobseekers from coming to the UK, while the pipeline of supply from UK universities remains weak (Ascentor, 2020). This will pose some challenges for businesses operating on an all-island basis and has the potential to impact on Northern Irelands competitiveness with its near neighbour.

InfoSecurity (2019a) notes that experts and IT security professionals have warned that Brexit could have a "chilling" effect on the UK's cyber security industry, by making cross-border intelligence sharing harder, and impacting jobs. If EU countries develop attractive hubs of cyber security expertise it's only likely to make the availability of cyber talent in the UK worse.

According to the European Parliament, the UK is a key partner when it comes to fighting terrorism in Europe. It has been, the 2nd biggest contributor to Europol information systems. Michel Barnier, the EC's top Brexit negotiator told attendees at the Web Summit in Lisbon in November 2019 that the EU and UK must join forces after Brexit to fight cyber-threats. "Our new partnership should include the exchange of information on cyber incidents, attackers' techniques, threat analysis and best practice, including when those target the correct functioning of democratic systems," Barnier said. "Crucially, we need to have capacity to respond jointly to such attacks." Despite this, after 20 years of involvement, the UK no longer has a place on the team that manages Europol. New arrangements for a new partnership after the transition period have yet to materialise (Ascentor, 2020).

The next section of this report showcases the results of the V-LINC analysis conducted on the specialisations of cyber firms in the South West of Ireland and Northern Ireland, which are connected to the cluster organisations - Cyber Ireland and NI Cyber respectively. Each cluster organisation was asked to reach out to a sufficiently reflective mixture of MNC and indigenous players with cyber security operations from their cluster. The size of these organisations ranged from Micro (< 10), Small (< 50), Medium (< 250) and Large enterprises (250+ employees). Eleven respondent firms were interviewed in the South West of Ireland and ten firms were interviewed in Northern Ireland (firms are listed in the NI Cyber and Cyber Ireland individual reports). The report presents the findings of the V-LINC analysis of the Cyber Ireland and the recommendations for that ecosystem followed by the NI Cyber ecosystem and its associated recommendations. Synergistic recommendations are then proposed from an all island ecosystem perspective aimed at enhancing north-south collaboration.

## V-LINC HIGHLIGHTS – CYBER IRELAND (SOUTH WEST)

Irish Tech News (2019) reports that Ireland has world class potential to become a global cyber security centre of excellence, the sector employs over 6,500 people and includes many of the world's top security firms. The V-LINC methodology has been applied to a sample of 11 cyber security firms based in the South West, a selection of Micro, Small, Medium and Large firms (AT&T Cyber Security, Cork Cyber Sec SME, Cyberlink Security, eSentire, JRI America, McAfee, McKesson, Qualcomm, Sophos, Trend Micro and UTRC). Thirteen face to face meetings were held with company personnel to gather information on 379 strategic relationships respondent firms (RFG[5]) engage in. Figure 3 displays these linkages geographically.

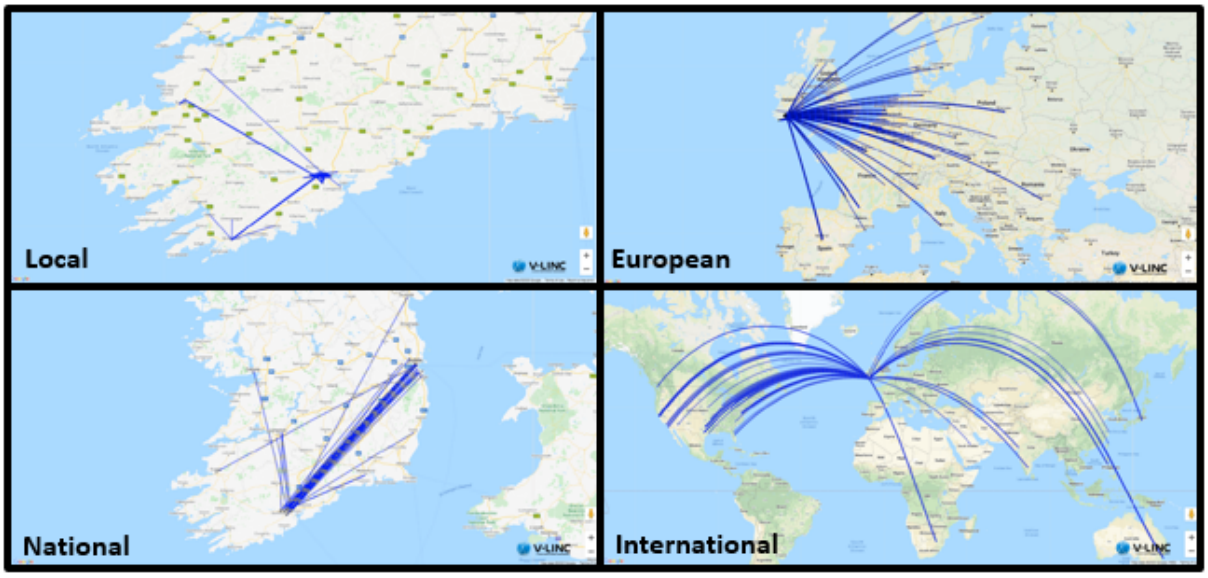


**Figure 3: South West Respondent Firm Group (RFG) Cyber Linkages by Geographic Scope.**

Cyber Ireland, hosted at CIT and supported by IDA Ireland and Enterprise Ireland, brings together the triple-helix to represent the needs of the cyber security ecosystem. It aims to enhance the innovation, growth and competitiveness of Ireland's cyber security ecosystem to: (1) Build the Community through promotion & supporting cross-industry collaboration; (2) Ensuring a sustainable pipeline of Cyber Security Talent & Skills; (3) Enhance collaborative R&D between industry and academia and (4) Support Irish SMEs & Start-ups to grow and export globally from Ireland. Since its launch in May 2019, there are over 170 member organisations, 160 of which are from industry.

[5] The term RFG relates to the Respondent Firm Group of the 11 companies who participated in the V-LINC analysis in tandem with Cyber Ireland in the South West.

Cyber Ireland has been showcased as a model for good practice in cluster development in the following strategies and programmes: Future Jobs Ireland 2019, South West Regional Enterprise Plan to 2020, Regional Spatial & Economic Strategy for the Southern Region, and via EU funded ecoRIS3 Interreg Europe Project, and ERASMUS+ International Credit Mobility.

## HIGHLIGHTS OF RESULTS

- Most frequent linkages are in Outputs, which account for 29% of linkages reported; followed by Industry Association (13%), Training (12%) and Specialist Services (12%).
- 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.
- In regard to customers, cyber firms based in the South West report that 95% of Output linkages are reported outside Ireland, with 54% destined for the European marketplace and 41% for International markets.
- Regarding Inputs, 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 there are no local input linkages, with 100% reported at National, European and International scopes.
- 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.
- Most of the Training (64%), Specialist Service (53%) and Research & Development (44%) linkages are recorded with Local organisations, such links are not viewed as important to respondents as over 40% are reported in the Low and Tenuous bands for each category.
- In terms of the key connectors identified in the Cyber Security sector in the South West (Figure 4), 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/Medium bands with 92% and 77% respectively. Other Key Connectors include UCC, it@cork, Cyber Ireland and Cork Chamber.


**Figure 4: Key Connectors in the South West of Ireland Cyber Security Sector.**

## 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. Note: All tables referred to below are found in the Cyber Ireland V-LINC Analysis.

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 5) 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.

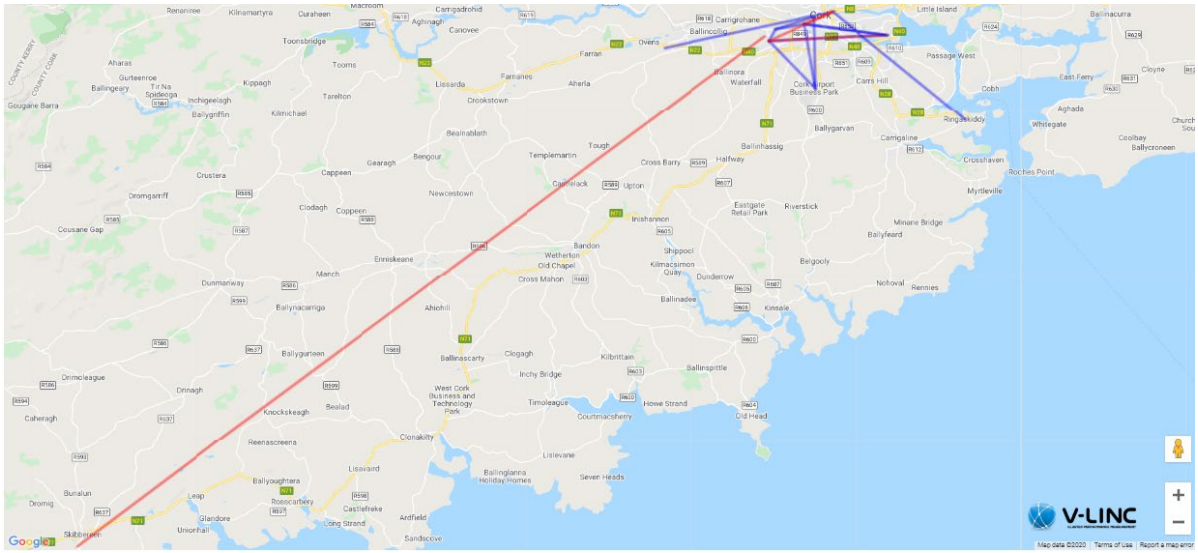


**Figure 5: Local R&D linkages in the South West cyber security sector.**[6]

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

[6] 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.

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 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. Cyber Ireland could be a central partner in developing and implementing 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 also a priority issue for the RFG. At present, there is 0% unemployment in cyber security roles worldwide, with 3.5 million unfilled jobs predicted by 2021[7], resulting in increasing global competition for talent and investment. A global study[8] from Enterprise Strategy Group and Information Systems Security Association 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%) and "a lack of adequate cyber security staff" (22%).

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.

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 6) 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.

[7] https://cybersecurityventures.com/jobs/
[8] http://www.prweb.com/releases/2017/11/prweb14899778.htm

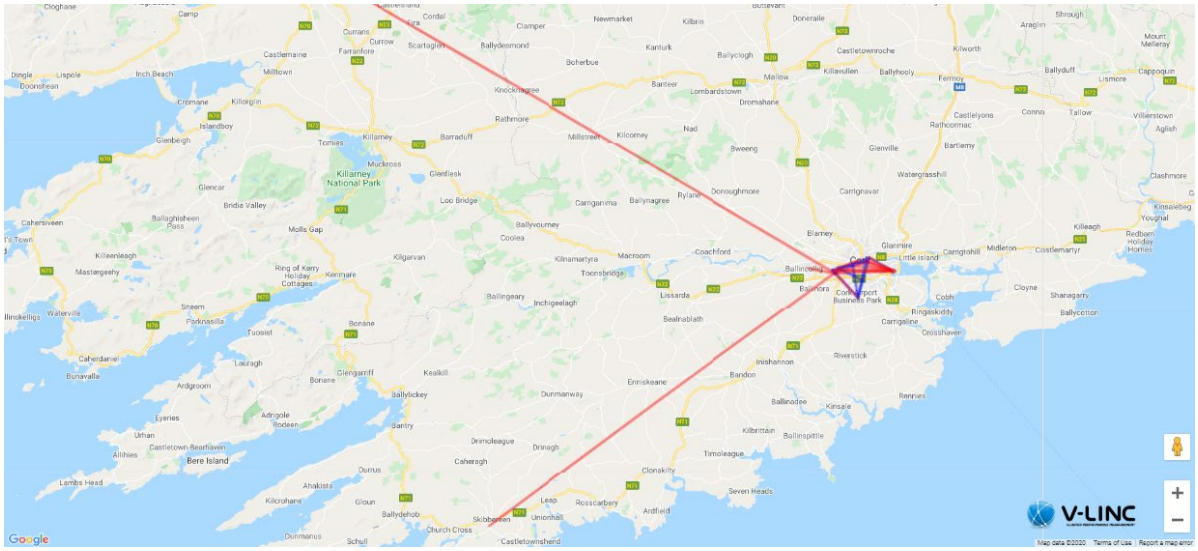


**Figure 6: Local Research & Development and Training linkages in cyber security Northern Ireland.**[9]

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.

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:

[9] 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.

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 [10] 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.

[10] 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[11] - 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.

This Cyber Ireland V-LINC Analysis report was written and compiled by Cork Institute of Technology in collaboration with Cyber Ireland. The authors wish to express their gratitude for the guidance, support and insights on the cyber sector in the South West of Ireland from the member firms of Cyber Ireland, IDA Ireland and Enterprise Ireland.

The full report can be downloaded from: http://www.v-linc.com/mappingthecyberisland

[11] http://be-wiser.eu/

## V-LINC HIGHLIGHTS – NI CYBER (NORTHERN IRELAND)

fDi Market Intelligence (2020) recognises Northern Ireland as the number 1 international investment location for US cyber security development projects. Over 75 cyber firms operate in Northern Ireland, employing almost 1,700 people, generating over £70,000,000 in salaries annually (Computer Weekly, 2019), with a target of having 5,000 employees in cyber by 2030 (NDNA, 2020). V-LINC methodology has been applied to a sample of 10 cyber firms in Northern Ireland, a selection of Micro to Large firms (Allstate, Ampliphae, Ansecia, B-Secur, Cygilant, Cynash, Kainos, Liberty IT, Skurio and Vertical Structure). Fourteen face to face meetings were held with personnel to gather information on 251 strategic relationships respondent firms (RFG[12]) engage in. Figure 7 displays these linkages geographically.

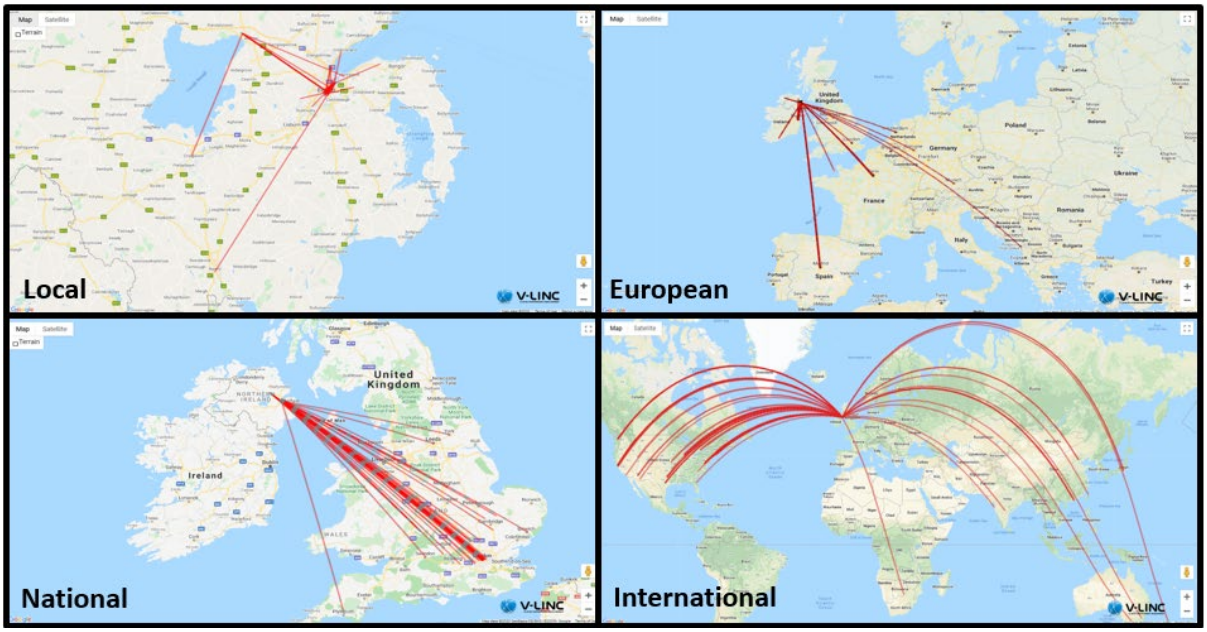


**Figure 7: NI Cyber Respondent Firm Group (RFG) Linkages by Geographic Scope.**

Cyber is an important sector for its growth and cross-cutting technologies which support growth and innovation in other sectors. Critical support elements in NI include Queens University Centre for Secure Information Technologies (CSIT) and Ulster University's Artificial Intelligence; Cognitive Analytics Research Lab (CARL); Intelligent Systems and Pervasive Computing research groups and centres. The Digital Catapult Centre Northern Ireland, is a shared site to drive innovation and connect industry and academia.

[12] The term RFG relates to the Respondent Firm Group of the 10 companies who participated in the V-LINC analysis in tandem with NI Cyber Ireland in Northern Ireland.

## HIGHLIGHTS OF RESULTS

- The most frequent linkages are in Outputs, 40% of all linkages reported; followed by Training (12%) and Inputs (10%).
- Local linkages make up the largest proportion (32%) of all linkages reported, the remaining 68% being divided between National (24%), European (12%) and International (31%).
- In regard to customers, cyber firms based in Northern Ireland report that 86% of output linkages are outside Northern Ireland, of which 23% is destined for the UK, a further 17% for the European marketplace and 46% Internationally.
- Regarding Inputs, 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 there are no local input linkages, with 100% reported at National, European and predominantly International (65%) scopes.
- It is reported that Outputs (59%) are rated of highest business impact by respondents, followed by Training (42%) and Inputs (38%) with the largest proportion occurring in the 'High' business impact band.
- 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.
- European linkages represent the least populous geographic scope, although 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, of input and output linkages.
- In terms of the key connectors identified in the cyber security sector in Northern Ireland (Figure 8), there are strong linkages to industry associations, government agencies, and research and education institutions. The standout linkages for the RFG are with NI Cyber, Invest Northern Ireland and CSIT, with the majority of linkages to these organisations in the High and Medium bands.


**Figure 8: Key Connectors Northern Ireland Cyber Security Sector.**

## RECOMMENDATIONS

Having reviewed the Cyber Security: A Strategic Framework for Action 2017-2021[13] and UK National Cyber Security Strategy 2016-2020[14] in tandem with the results of the V-LINC analysis, the following policies aim to develop the Northern Ireland cyber security sector. Note: All tables referred to below are found in the NI Cyber V-LINC Analysis.

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 9).

[13] https://www.finance-ni.gov.uk/sites/CSSF2017-2021.pdf
[14] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

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[15] 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.

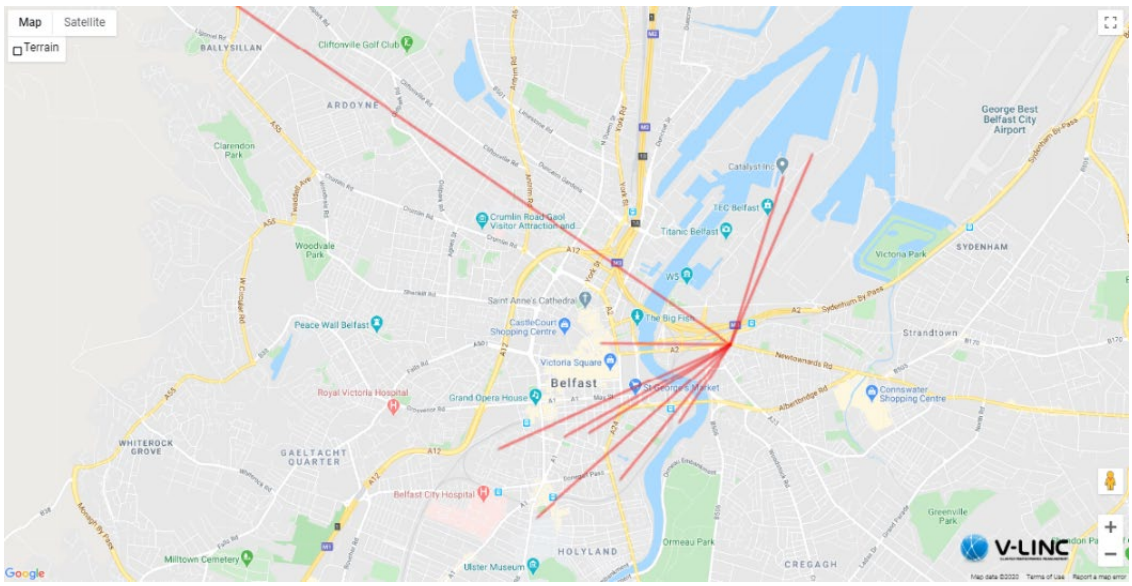


**Figure 9: Local Industry Association linkages in the cyber security sector.**

[15] https://www.investni.com/collaborative-growth-programme

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 10), 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.

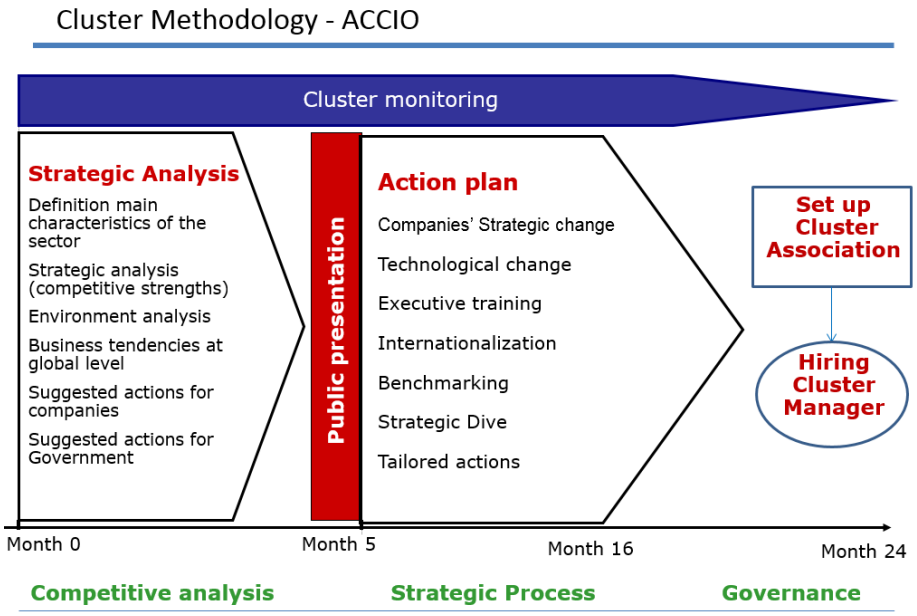


**Figure 10: The Catalonia Cluster Development Strategy process utilised by ACCIÓ**[16]

At present, NI Cyber is supported through Invest Northern Ireland's Collaborative Growth Programme – Phase 1, which has funded the appointment of an independent facilitator who is carrying out a scoping study to investigate the potential to establish a Northern Ireland cybersecurity collaborative cluster over a period of six months. Depending on the outcome of Phase 1, additional funding (up to a maximum of £170,000) may be available to support the implementation of phase two.

[16] ACCIÓ is the Catalan Agency for Competitiveness. This method was presented by Joan Martí Estévez, Director of Cluster Development ACCIÓ, at the Cluster Seminar Series in CIT, September 2015.

**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 11).

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 locally 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' reportP7 (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.

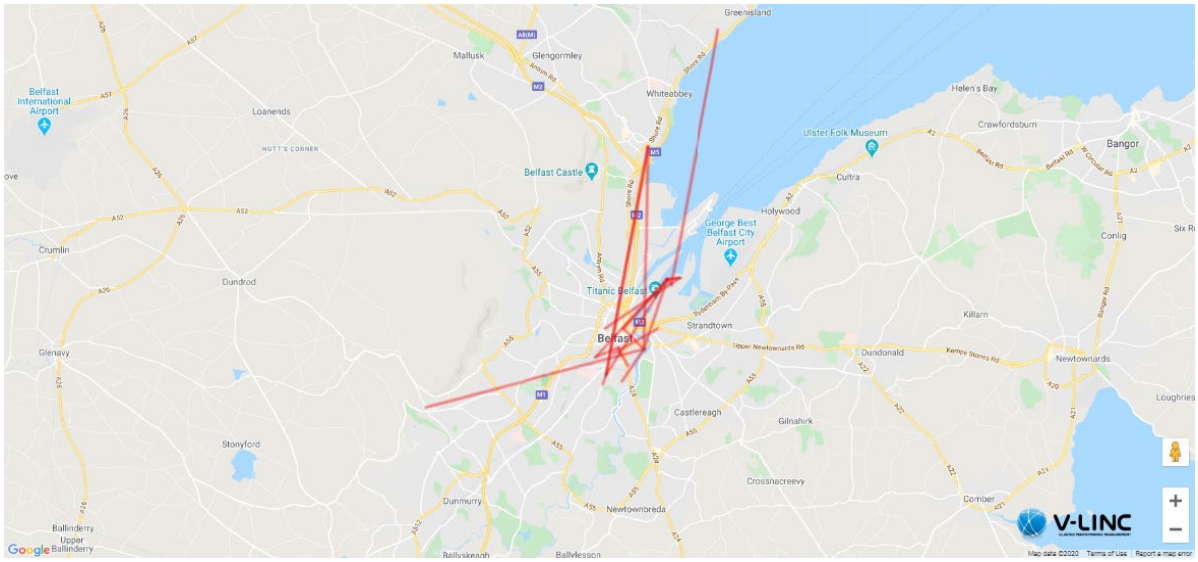


**Figure 11: Local Research & Development and Training linkages in cyber security Northern Ireland.**

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 12). 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 12: European & International Output Linkages Operated by 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's[17] 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.

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.

[17] Cyberforum is the largest high-tech cluster in Germany with over 1000 members http://www.en.cyberforum.de/home

This NI Cyber V-LINC report was written and compiled by the Cork Institute of Technology in collaboration with NI Cyber and CSIT. The authors wish to acknowledge the contributions of Judith Millar, Centre for Secure Information Technologies (CSIT) at Queens University Belfast; Linda Jamison, Invest Northern Ireland; Dr Krystal Miller, University of Ulster and Scott Carson, Department for the Economy. Furthermore, the guidance, support and insights on the cyber sector in Northern Ireland from the member firms of NI Ireland helped to shape and support the report.

The full NI Cyber V-LINC Analysis can be downloaded from: http://www.v-linc.com/mappingthecyberisland

## MAP OF THE CYBER ISLAND.

As part of the Mapping the Cyber Island Report, it was pertinent to include a map of the key actors across the island of Ireland within the cyber security sector.

The companies included in Figure 13, are the member/partner organisations of Cyber Ireland and NI Cyber. It is apparent there are concentrations of activity in Belfast, Dublin, Cork, Limerick and Galway. The 224 companies on the map are categorised by pure-play Cyber Security (102), ICT & Software (53), Professional Services (22), Academia (10), Government (8), Financial Services (12), Healthcare (5), Telecoms (2), and Other (10).

The Cyber Island Map is available on the V-LINC webpage at: http://www.v-linc.com/mappingthecyberisland. Cyber organisation details can be found by selecting the organisation icon, which opens an information box displaying name, address, industry sector, primary cyber security operations and website.


**Figure 13: Mapping the Cyber Island – Cyber Island and NI Cyber Participants across Ireland.**

Regarding linkages between the Cyber Ireland Cluster and the NI Cyber Cluster there are three connections between Cork and Northern Ireland – these connections are: 2 Research & Development and 1 Government Agency linkage. These three linkages are of (1) Medium and (2) Low business impact.

Looking at linkages from NI Cyber to the Republic of Ireland these are more numerous. There are two connections to the Cyber Ireland Cluster in Cork, 1 = Industry Association and 1 = Output, 1 in the High and 1 in the Medium business impact band. Another 11 linkages exist from firms in the North with connections into Dublin (9) and Donegal (2), across Industry Association (1), Output (9) and Training (1), these connections are 6 in the High, 4 in the Medium and 1 in the Low business impact bands.

## OPPORTUNITIES FOR COLLABORATION

As part of the V-LINC interviews additional questions were included to ascertain current trade levels and appetite for cross border collaboration.

***Q1: Have you any customers in Northern Ireland or the Republic of Ireland? If yes, what is the value of this business relative to your overall turnover?***

| % Turnover | Cyber Ireland firms % Turnover in Northern Ireland | NI Cyber firms % Turnover in Republic of Ireland |
|---|---|---|
| 0% | 55% | 50% |
| 0-10% | 36% | 40% |
| 10-20% | 9% | 0% |
| 20-30% | 0% | 0% |
| > 30% | 0% | 10% |
| Total (n) | 11 | 10 |

**Table 2: Percentage of turnover reported in Northern Ireland or the Republic of Ireland by cross border firms who participated in the V-LINC analysis.**

In Table 2, five firms from the Cyber Ireland respondent firm group report turnover in Northern Ireland, the majority in the 0-10% of turnover band. Similarly, five firms from the NI Cyber respondent firm group report turnover in the Republic of Ireland – with this being a key market for one participant who has >30% of their annual revenue from customers in Ireland.

***Q2: Are you interested in cross border collaboration with stakeholders from Northern Ireland or the Republic of Ireland? If yes, what type of collaboration are you interested in?***

| Collaboration Type | Cyber Ireland firms' interest in collaboration (type) in Northern Ireland | NI Cyber firms' interest in collaboration (type) in Republic of Ireland |
|---|---|---|
| Study Visits | 73% | 10% |
| All Island Cross Border Training | 36% | 20% |
| Networking | 73% | 70% |
| Conferences | 91% | 60% |
| Workshops | 45% | 30% |
| Cross Border Knowledge Transfer | 45% | 20% |
| Other | 18% | 40% |

**Table 3: Percentage of respondents interested in different types of cross border collaboration.**

Table 3 shows that there are slight differences between the respondent firm groups from Cyber Ireland and NI Cyber regarding different types of collaboration they would be most interested in.

For the respondents from the South West of Ireland (Table 3), cross border conferences were of most interest with 10 out of 11 (91%) of respondents interested in participating/attending. This was followed by cross border study visits and networking with 73% of respondents interested in visiting Belfast to look at the resources there, CSIT and the Digital Catapult were mentioned by a number of respondents and networking with companies in Northern Ireland. It cannot be underestimated the focal point such R&D and enterprise support incubators can provide for a sector in a region. It was also interesting to note that Business Collaboration / Pitching / Elevator Pitches were mentioned in the 'other category'.

Respondents in Northern Ireland (Table 3) suggest cross border networking opportunities were of most interest with 7 out of 10 interested. This was followed by cross border conferences with 60% of respondents interested in participating/attending in such cross border events. The third most popular type of collaboration respondents would like to pursue with counterparts in the Republic were listed in the 'other category'. These included: matchmaking, collaborative partnerships and clinical and University research connections.

It seemed evident from the interviews that the respondents in Northern Ireland were not aware of a focal point for the cyber sector in the South or of an academic research centre of world class status like CSIT – that has built up credibility over years of scientific research and is recognised internationally. This point resonates closely with the V-LINC Cyber Ireland Analysis and the policy recommendations there where industry academia linkages are missing a central point of contact – Cyber Ireland can fill this void in the interim period, but longer term a National Cyber Research Centre is key to addressing and progressing the R&D agenda and the skills gap.

The possibility of the development of an all island research centre in the area of Artificial intelligence / Cyber Security is proposed in an SFI paper North-South Future Initiatives published in 2019 and in the 'New Decade New approach' document which was published by the Irish Tánaiste and Secretary of State for Northern Ireland to restore devolved government in Northern Ireland in January 2020.

## CONCLUSIONS

The Mapping the Cyber island project is a useful first step in supporting the strategic development of Cyber Ireland and NI Cyber as it provides:

- An overview of the cyber focused firms on the Island of Ireland (Figure 6) which is available online @ http://www.v-linc.com/mappingthecyberisland.
- Visualisations of the linkages and connections forged by participants of Cyber Ireland (Figure 2) and NI Cyber (Figure 4) clusters.
- Dedicated policy recommendations based on current policies at regional and national levels along with the V-LINC analysis results in the South West of Ireland and Northern Ireland. These can be implemented by Cyber Ireland and NI Cyber respectively.
- An articulation of the types of collaborative supports of interest to firms operating in the South West of Ireland and Northern Ireland to allow them to connect (Table 3).

It is obvious from the above elements, and their associated reports that several shared issues are of great importance to members of Cyber Ireland and NI Cyber.

1. **The critical skills shortage:** skills is a major issue in both territories with InfoSecurity (2019b) reporting that global IT security skills shortages have now surpassed four million, according to (ISC)$^2$. The certifications organization compiled its latest Cybersecurity Workforce Study from interviews with over 3200 security professionals around the world. The number of unfilled positions now stands at 4.07 million professionals. With the shortage of skilled workers in the industry in Europe having soared by more than 100% over the same period, from 142,000 to 291,000.

   Based on the ever-increasing need for cyber skills in the Republic of Ireland and the ambitious target of having 5,000 employees in the cyber security sector in Northern Ireland by 2030 (NDNA, 2020), there are opportunities for Cyber Ireland and NI Cyber to collaboration in this space. Collaborating on elements such as (i) cyber security skills surveys for members, (ii) breaking down barriers between academic institutes to help them collaborate more, (ii) the running of short courses to address key industry challenges by the clusters and (iv) promotion of cyber security careers to primary and second level students to increase the flow into the talent pipeline.

2. **Support the development of industry and academic research and development linkages:** It is evident that R&D linkages are one of the least populous linkage categories in the study in both Ireland where just 36 linkages are reported and in Northern Ireland where just 15 linkages are reported. These findings are extremely surprising for such a high-tech industry segment. However, they can be explained through the fact that firms are operating at the cutting edge of these technologies and dealing with new threats on a daily basis. However, if we are to stay protected and ahead of the curve strengthening collaborative opportunities between industry and academia is paramount.

   There are opportunities for Cyber Ireland and NI Cyber to partner to run a co-operation project programmes where several firms (including at least one SME) could partner with a number of academic institutes to strategically differentiate themselves. Perhaps the InterTradeIreland Synergy Programme could kick start or be utilised to co-develop this co-operation programme. Another option would be to utilise the new cyber security priority area of the US-Ireland R&D Partnership to connect academics with industry locally, and through the Department for the Economy in Northern Ireland and Science Foundation Ireland (SFI) in Ireland utilise the US-Ireland R&D Partnership connect scientists and engineers across the three jurisdictions to increase level of collaborative R&D.

   It seems such an approach is supported in the 'New Decade New approach' document which was published by the Irish Tánaiste and Secretary of State for Northern Ireland to restore devolved government in Northern Ireland in January 2020. The Irish Government commitments to collaboration under the section on research and innovation, when the document states: "we look forward to developing proposals for an enhanced North/South programme of research and innovation, in cooperation with the NI Executive through the NSMC and relevant agencies and stakeholders, North and South".

3. **Facilitate B2B linkages:** One of the key findings with respondents from Cyber Ireland and NI Cyber was the low numbers of Industry Peer linkages, the least numerous of the categories overall in both analyses. This indicates difficulties that the respondents 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 Cyber

Ireland respondents report 88% of their 25 Industry Peer linkages at European and International levels, and that over 75% of these connections are reported in the High and Medium impact bands. Similarly, the numbers of Industry Peer linkages reported by NI Cyber respondents at European and International levels whilst smaller (n=5), and report over 75% of these connections in the High and Medium impact bands.

The question is why more trusted Industry Peer linkages are not being developed across the island of Ireland? Perhaps the answer lies in the stage of development of the cyber security sector across the island, where capacity has been built by numerous foreign multinational firms who have located themselves across the Republic of Ireland and in Belfast in Northern Ireland. These firms are growing quickly and seeking talent, at the same time indigenous start-ups are growing and spinning out of higher education institutes to rapidly fill the security needs of other sectors across the island who need to keep their data, transactions and customer information safe and secure. Perhaps this growth phase coinciding with the fight for talent to fuel this growth, is limiting the ability of trust and collaboration to be developed between these companies.

If clustering in the cyber security sector is to be successful, these type of B2B linkages based on trust and cooperation need to be developed to allow companies to develop and grow and tackle shared problems together. There is an opportunity through the InterTradeIreland Synergy programme to jumpstart the development of the required market focused B2B connections in both Ireland and Northern Ireland through a roll out of the dealbroker programme and cyber brokerage events, which could be managed in tandem by Cyber Ireland and NI Cyber. These could take several 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 development agencies to reach new markets.

Finally, there are opportunities to roll out the V-LINC analysis to additional members of the Cyber Ireland and NI Cyber clusters, perhaps in Dublin and Galway to support on-going strategic development and analyse further North-South collaborations perhaps on the back of some of the recommendations being implemented from this report.

## BIBLIOGRAPHY


- Ascentor (2020), 'Cutting through the confusion: Cyber security after Brexit,' February. Available Online @ https://www.ascentor.co.uk/2020/02/cybersecurity-after-brexit/
- Bathelt, H., Malmberg, A. and Maskell, P. (2004), 'Clusters and knowledge: local buzz, global pipelines and the process of knowledge creation,' Progress in Human Geography, 28 (1): 31-56.
- Borgatti, S.P. and Halgin, D.S. (2011), 'On Network Theory,' Organization Science, Vol. 22, No. 5, September–October, pp. 1168–1181
- Boschma, R. (2005), 'Proximity and Innovation: A Critical Assessment,' Regional Studies, 39 (1): 61-74.
- 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.
- Christensen, T., Lämmer-Gamp, T. and Meier zu Köcker, G. (2012), Let's make a perfect cluster policy and cluster programme, Berlin/Copenhagen: VDI/VDE.
- 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.UK_Cyber2020_Report.pdf.
- Dillman, D., Smyth, J., Leah-Melani, C. (2014), Internet, Phone, Mail and Mixed-Mode Surveys: The Tailored Design Method, 4th edition, John Wiley: Hoboken, NJ.
- Donaldson, S., Shah, J.N., Crozier, D., and Furnell, S. (2020) 'UK Cyber Security Sectoral Analysis 2020: Research report for the Department for Digital, Culture, Media and Sport', January 2020. Available Online @ https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020.
- ENISA (2017), 'ENISA overview of cybersecurity and related terminology,' Available Online @ www.enisa.europa.eu.
- Fahy, J. (2001), The Role of Resources in Global Competition, London: Routledge.

- fDi Markets Intelligence (2020), 'Digital Economies of the Future 2019/20 – the results.' Available Online @ https://www.fdiintelligence.com/Digital-Economies.
- Freeman, R.E. (1999), 'Response: Divergent Stakeholder Theory,' The Academy of Management Review, Vol. 24, No. 2 April, pp. 233-236.
- 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,' Published in December by the National Cyber Security Centre, Available Online @ https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf.
- Hetherington, G., Magennis, E., and Victor, K., (2019), 'Cluster Policy in Northern Ireland: Best practice and findings from consultation across three sectors,' Ulster University, Economic Policy Centre, December 2019. Available online @ https://www.economy-ni.gov.uk/sites/default/files/publications/economy/Cluster-Policy-in-Northern-Ireland.pdf.
- Hobbs, J. (2010), A Framework for Analysis of Spatial Specialisations of Industry, PhD thesis, Cork Institute of Technology.
- 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.
- Infosecurity (2019a), 'Brexit is Having a Chilling Impact on UK Cybersecurity Skills,' March, Available @ https://www.infosecurity-magazine.com/infosec/brexit-uk-cybersecurity-skills-1-1/.
- Infosecurity (2019b), 'Cybersecurity Skills Shortage Tops Four Million,' November, Available online @ https://www.infosecurity-magazine.com/infosec/brexit-uk-cybersecurity-skills-1-1/.
- 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/.
- Leydesdorff, L. (2012), The Triple Helix of university–industry–government relations. Encyclopaedia of creativity, innovation, and entrepreneurship, New York: Springer.

- Lublinski, A. E. (2002), Concepts for Cluster-Identification with an application to an alleged aeronautics cluster in Northern Germany, PhD thesis, University of Hamburg, Hamburg.
- Marshall, A. (1890), Principals of Economics, London: Macmillan.
- 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/pressrelease/New-Decade-New-Approach.pdf.
- Owen-Smith, J. and Powell, W. W. (2004), 'Knowledge Networks as Channels and Conduits: The Effects of Spillovers in the Boston Biotechnology Community,' Organization Science, 15 (1): 5-21
- 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.
- Rosenfeld, S. A. (2002), 'Creating smart systems: A guide to cluster strategies in less favoured regions,' European Union-Regional Innovation Strategies, Available at: http://www.rtsinc.org.
- Singh, J. (2005), 'Collaborative Networks as Determinants of Knowledge Diffusion Patterns', Management Science, 51 (5):756-770.
- Sölvell, Ö. and Protsiv, S. (2008), Cluster strengths and regional innovation, Stockholm: Stockholm School of Economics.
- Sölvell Ö., Ketels, C. and Lindqvist, G. (2009), 'The European Cluster Observatory: EU Cluster Mapping and Strengthening Clusters in Europe,' Center for Strategy and Competitiveness, available at: www.europe-innova.eu.
- Tallman, S. and Phene, A. (2007), 'Leveraging knowledge across geographic boundaries,' Organization Science 18: 252–260.
- Whittington, K. B., Owen-Smith, J. and Powell, W. W. (2009), 'Networks, propinquity and innovation in knowledge-intensive industries,' Administrative Science Quarterly, 54: 90–122.