CYBER RESILIENCE ALLIANCE

A Science and Innovation Audit Report sponsored by the Department for Business, Energy and Industrial Strategy

Department for Business, Energy & Industrial Strategy

Review led by:

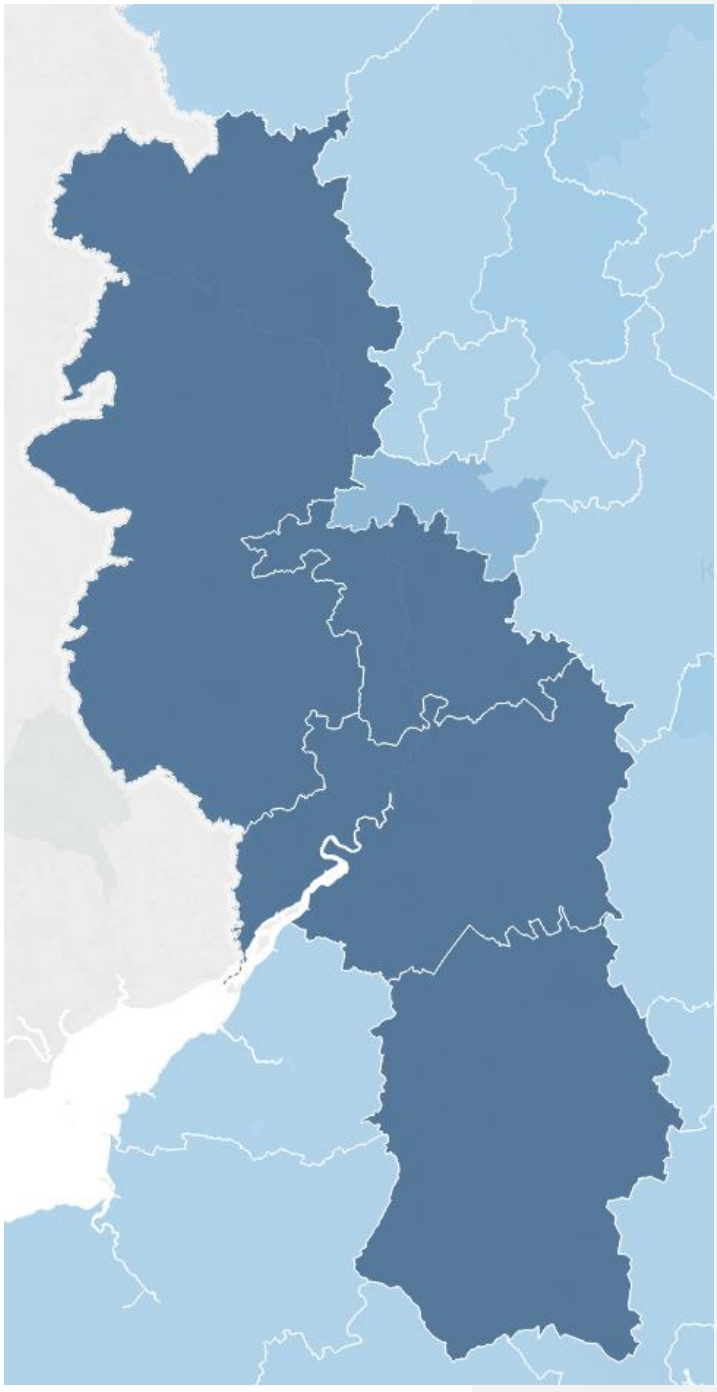
Worcestershire Local Enterprise Partnership

gfirst LEP growing gloucestershire

Swindon & Wiltshire Local Enterprise Partnership

The Marches Local Enterprise Partnership Herefordshire - Shropshire - Telford & Wrekin

Skylon Park



RSM

TABLE OF CONTENTS

1. ACKNOWLEDGEMENTS

Acknowledgements from Cyber Resilience Alliance Steering Group:

This report is sponsored by the Department for Business, Energy and Industrial Strategy (BEIS) and is produced on behalf of the Cyber Resilience Alliance, a consortium of over a hundred commercial, private, public, and voluntary organisations from across Worcestershire, Gloucestershire, The Marches (Shropshire, Herefordshire, and Telford and Wrekin), and Swindon and Wiltshire.

The Cyber Resilience Alliance is committed to endorsing and supporting the implementation of this Audit.

This report has been facilitated by the ongoing dedication of the Cyber Resilience Alliance Steering Group and its advisors. Sam Donaldson and Matt Rooke (RSM Economic Consulting) have also supported extensively in the collation and reporting of the region's economic and skills base. The Steering Group also provide thanks to Technopolis for their support in providing bespoke analytical support.

Throughout this process, the Science and Innovation Audit received written or verbal evidence from over sixty leading members of business, academic and public bodies. These contributions are greatly appreciated by the Cyber Resilience Alliance, and have been a valuable call to action for the region.

Steering Group Membership:

Gary Woodman: Worcestershire LEP

Gary is tasked with driving forward Worcestershire LEP and leading an Executive Team to support the WLEP's ambitions and delivery of the WLEP business plan. From his former role as Head of Policy and Education at Herefordshire and Worcestershire Chamber of Commerce, he has brought with him a wealth of business insight and networks as well as considerable experience of Government policy and delivery. Educated at the University of Wales, Cardiff, where he obtained his degree in Leisure and Recreation Management, and the University of Gloucestershire, where he studied for his postgraduate diploma in Business Administration, he previously worked for Gloucestershire County Council's market towns and economic development arm, overseeing regeneration.

Nicola Whiting: Titania

Nicola Whiting is an experienced Chief Operations & Strategy Officer with a strong history of working in Cyber Security / InfoSec. Specialising in enterprise security automation software (self-healing networks), business development, trust-based selling and neuromarketing.

An advocate for Autism and Women in Cyber, she provides government level advice on Diversity and writes for publications such as The Huffington Post, Defence Contracts Bulletin, Defence News Online and Signal. A well regarded public-speaker, keynote topics include "The Rise of Automated Attacks", "The Future of Automated Cyber Defences" and "Hacking the Human Brain".

In 2017 Nicola was named by SC Magazine as one of the Top 20 most influential women working in cyber security.

Professor Ian Oakes: University of Wolverhampton

Over the last 20 years, Professor Oakes has held a number of senior management posts in higher education before joining the University of Wolverhampton in 2008 as Pro Vice-Chancellor with responsibility for the University's research and enterprise agenda and developing the growing knowledge transfer arena at regional, national and international levels. More recently he was promoted to the role of Deputy Vice-Chancellor as well as Chief Executive of University of Wolverhampton Science Park.

Professor Kamal Bechkoum, Professor of Computing, is Head of The School of Business & Technology at The University of Gloucestershire. He is a Gloucestershire Commissioner for Cyber, Science and Innovation and the University lead of a £3m Cyber Security project, working with other organisations to produce highly skilled cyber professionals in Gloucestershire and beyond. Professor Bechkoum has also worked at Cranfield, De Montfort, Wolverhampton, Derby, and Northampton where he was Executive Dean of the School of Science and Technology with university executive responsibility for research and enterprise and intellectual capital. He holds a PhD in Software Techniques for Computer Aided Engineering from the University of Cranfield, UK and is a Fellow of the British Computer Society and a Chartered IT Professional.

Professor Richard Benham is the world's first formal Professor of Cyber Security Management and lectures at Coventry Business School and at the UK's National Cyber Skills Centre where he is Professor in Residence. He is also a Visiting Professor in in Cyber Security Management at The University of Gloucestershire and previously in Policing at Staffordshire University. Outside of the UK, Prof Benham is a SWIFT Institute Scholar and speaks at one of the World's leading Business schools, IMD in Switzerland. In 2013 he published "The Cyber Ripple Theory®" which is widely recognised as the World's first Cyber Management Theory and includes the human elements of Cyber Security. In 2017 he was chosen to join the DL100 and was nominated for UK Digital Champion of the Year. He is currently the Digital Champion for the South West.

Mark Pearce: Skylon Park: Mark is the Managing Director of Hereford Enterprise Zone Limited, a private/public partnership company charged with catalysing business investment at Skylon Park, the only Enterprise Zone in the country with a defence and security focus. In his 6 years at Skylon Park, over 37 acres of land has been sold, 41,000 sq m of new workspace built or committed, 38 businesses moved in and over £20m of private sector investment secured, with more sales and projects in the pipeline. An economic development professional of nearly 30 years standing, Mark worked previously at the West Midlands Regional Development Agency, Advantage West Midlands (AWM) for over 10 years, latterly as Corporate Director. He oversaw significant investment into urban and rural regeneration in the West Midlands including longstanding Board representation at Hereford Futures, the £100m+ mixed use project that has transformed Hereford City Centre.

Dev Chakraborty: Gloucestershire LEP: Dev is currently the Deputy Chief Executive for GFirst LEP, Gloucestershire's Local Enterprise Partnership. Dev has over 25 years experience in marketing, sales and media roles in the South West, including 10 years of senior management and board level experience. Dev was part of the original team that launched Cornwall's award winning, commercial radio station, Pirate FM then becoming Managing Director of Star FM in Bristol. Immediately prior to his role at GFirst LEP he was a Business Guide at the Growth Hub working with high growth businesses across Gloucestershire.

Kathryn Jones: Marches LEP: Kathryn joined the Marches LEP team in October 2017 as Partnership Manager. She has a background in economic development and has managed international, regional and local business support projects, including research and development grant programmes and business growth initiatives. More recently, she has worked in the further and higher education sectors promoting the importance of skills development in driving economic productivity.

Colette Mallon: Swindon and Wiltshire LEP: Colette leads Business Engagement for the SWLEP. She has specific responsibility for building relationships with businesses, government, stakeholder organisations and other LEPs to support the delivery of the Swindon and Wiltshire Strategic Economic Plan.

2. FOREWORD

The UK is a globally leading digital economy, and our prosperity is reliant upon our ability to secure our businesses, data and networks from cyber threats. The Cyber Resilience Alliance region[1] consists of some of the UK's brightest minds and cutting-edge technology addressing cyber security challenges every day. As cyber-attacks become more frequent and more damaging, our region offers the talent and resources that lead the way in supporting the UK's efforts to be one of the the most secure, capable, and cyber resilient countries in the world.

We are home to over a hundred businesses and organisations (and growing) active in cyber security product and solution development including large names such as Northrop Grumman, BT, Raytheon, BAE Applied Intelligence, Lockheed Martin, and Nationwide Building Society; highly regarded cyber security firms such as Anomali, Anon AI, and Titania; and rapid growth in innovative start-ups including PixelPin and Ripjar.

Outside of London, we are the UK's leading region in cyber security, with an estimated 5% UK market share, despite having 3% of the UK's population. However, our close-knit community has historically been rooted in securing the UK: during World War II the UK Government moved its radar technology to Malvern; which now holds the UK's largest cluster of cyber security firms. In 2001, QinetiQ, a major defence and security firm, was established through the privatisation of the Defence Evaluation and Research Agency (part of the Ministry of Defence), alongside the creation of the UK's Defence Science and Technology Laboratory (Dstl) in Porton Down. Over 5,000 of our community work in GCHQ in Cheltenham at the heart of UK security matters, and we also host the Ministry of Defence Joint Cyber Unit based in Corsham, and the Special Forces in Herefordshire.

This Science and Innovation Audit has helped to bring together our community of business, entrepreneurs, academics, policy practitioners, and defence, security and cyber expertise in a new way: to identify common strengths, challenges and opportunities for growth.

We are particularly strong in public administration, defence, security, health, and manufacturing. These are all industries that not only require cyber security solutions, but will actively drive the need for innovation, new products, and growth in the industry.[2]
Our people are ambitious and determined to cement the Cyber Resilience Alliance region as a leading place for UK and global cyber security practice helping to grow the region, secure the UK's assets, and to support cross-sectoral and cross-boundary initiatives that can create innovative, world-leading and secure products and services in the UK economy.

We have the skills, infrastructure, and resources in place to continue growing the sector, but we recognise the challenges ahead. That's why we are investing heavily in infrastructure, skills and talent, research and knowledge transfer, and focusing our efforts in making the region the leading location for cyber security firms outside London.

[1] Worcestershire, Gloucestershire, The Marches, and Swindon & Wiltshire LEPs.
[2] The UK Cyber Exports Strategy identifies the six most promising sectors for UK cyber security exports in 2018 (Government, Financial Services, Automotive (and Autonomous Vehicles), Energy and Critical National Infrastructure, Health, and Infrastructure)

SUMMARY REPORT

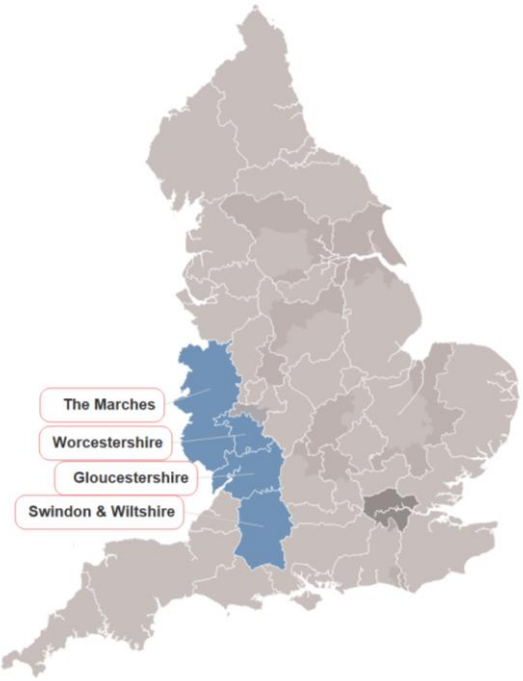
Introduction & Context

In Autumn 2015 the UK Government announced regional Science and Innovation Audits (SIAs) to catalyse a new approach to regional economic development. SIAs enable local consortia to focus on analysing regional strengths and identify mechanisms to realise their potential.

In Gloucestershire (GFirst), Worcestershire, The Marches (Shropshire, Herefordshire, and Telford and Wrekin), and Swindon and Wiltshire Local Enterprise Partnerships (LEPs), the **Cyber Resilience Alliance** was formed in 2017 to focus on our strength in cyber security. This report presents the results which includes broad-ranging analysis of the Cyber Resilience Alliance's capabilities, the challenges and the substantial opportunities for future economic growth.

The Region[3]

The Cyber Resilience Alliance region consists of four Local Enterprise Partnerships (LEPs), stretching from north of Shrewsbury to south of Salisbury (over 180 miles). The region spans more than 5,200 square miles (10.4% of England's total geography), with 2.59 million residents, of which 1.58m are aged between 16-64 (3.8% of the UK's working age population). At its heart, it includes the urban settlements of Worcester, Cheltenham, Gloucester, Hereford, Telford, Swindon and Shrewsbury which are well-connected to the rest of the country via strong rail links and the M5 motorway corridor that runs from Birmingham through to Bristol (through the centre of Worcestershire and Gloucestershire LEPs).



The region is synonymous with UK defence and security and is home to some of the world's largest defence firms (BAE Systems Applied Intelligence in Gloucester, Babcock in Swindon, and Lockheed Martin in Wiltshire). as well as the UK's highest levels of public security (Ministry of Defence in Corsham, Special Forces in Hereford, and GCHQ in Cheltenham).

[3] See Section 3: Introduction to the SIA Region

Within the Cyber Resilience Alliance region, we recognise the considerable **concentration of cyber skills within the population[4], largely due to proximity to GCHQ which in recent years has also encouraged a wide range of spin-outs and investment from cyber security organisations.**

The key to industrial success in the future is not just establishing cyber businesses. It is also about embedding cyber skills and principles of 'secure by design' into the existing industrial infrastructure. This will provide competitive advantage, and increase opportunities for employees to develop skills that make them and their business more attractive in a global market. We also recognise that skills being currently developed could be vulnerable to future automation, with a need to ensure there is a route to maximise high value skills and increase resilience moving forward.

This audit is therefore structured to test two main hypotheses:

1. There is a strong **concentration of skills in cyber security within the region, which can be used to embed cyber resilience through a wider industrial base,** including making a strong contribution to the growth of the UK's cyber security sector directly, and supporting industries within which their demand for secure solutions will incubate, support and grow the region's economy.

2. **Sustainable business needs to be competitive and trusted. Do traditional businesses do enough to understand and embrace cyber resilience, and how can they best invest accordingly?**

   The Audit will identify opportunities to build linkages between the strong regional cyber security expertise and the wider community.

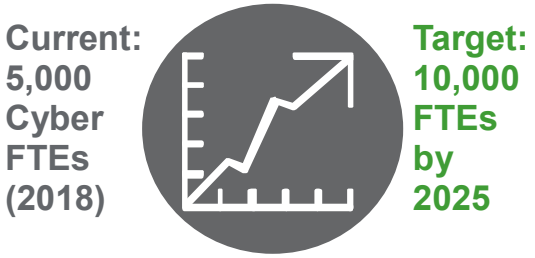
[4] See Section 4 Strengths and Innovation, and Section 5.2 Size and Scale of the Cyber Resilience Alliance Sector

Vision

To maximise the opportunities of the cyber security sector in the Cyber Resilience Alliance, we set out the following evidence-informed vision for the region.

Firstly, we want to double the size (measured by employment) of the cyber security sector in the region, aligning the potential of our people with high-value employment into firms that can be global leaders.

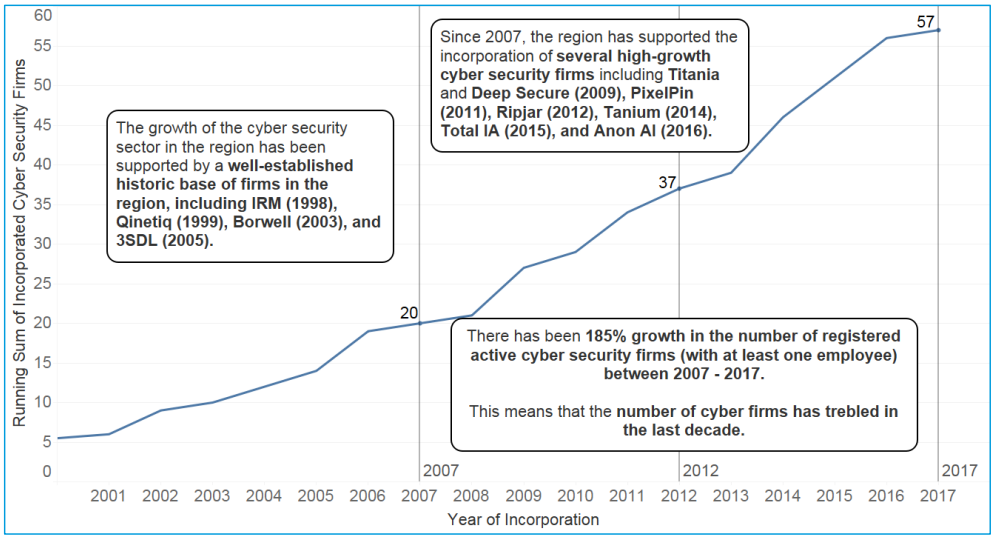
We will plan interventions in line with anticipated and sustainable growth (approximately 10% per annum).



By 2025, we aim to have 10,000 (FTEs[5]) employed in the sector.[6]

Secondly, this Science and Innovation Audit has confirmed many of the propositions set out within our Expression of Interest: the region is particularly strong in cyber security with respect to the number of firms (more than fifty cyber security firms[7]), and over a hundred organisations and firms actively shaping cyber security products, services and development. As a result, we want the region to be known nationally and internationally as the **UK's largest cluster of cyber security activity outside London.**

Registered Cyber Security Companies within the Region: A Rapidly Growing Sector…



Source: Bureau van Dijk

[5] Full Time Equivalent staff
[6] See Section 5.3 Employment Estimates and Projections
[7] DIT (2018) Cyber Security Export Strategy identifies c. 800 cyber security firms in the UK.

Thirdly, with this recognition, we want to ensure that the region continues to promote an entrepreneurial start-up culture & attracts new investment. As a result, by 2025, we estimate that the region's sector will contain more than one hundred active cyber security firms – and with further investment and support, this figure could be even higher, particularly given the attractiveness of the region (competitive operational costs for business, a growing talent pool, and strong clusters of cyber innovation). Further, we will endeavour to identify opportunities for firms in manufacturing, defence, automotive, financial services and other sectors to embrace cyber security as a core component in product development.

This aligns to the findings of this Audit that nominal R&D expenditure has increased within the West Midlands and South West since 2008 at twice the national rate (grown 43% between 2008-14 compared to 21% across the UK). In recognition of the rapid growth in BERD[8] in the region, and the potential for disruptive technologies to require cyber security solutions (particularly in advanced manufacturing and automotive), we will support cyber security firms to identify UK supply chain opportunities that can further grow R&D expenditure in the region, improving the quality and value of our strong manufacturing base.

Finally, we recognise there is a long-standing productivity gap in the region. GVA per capita in the region is £22,804 (2015). This means that productivity is 10% lower than the UK's GVA per capita (£25,351). Tech Nation (2017) identify an average advertised digital salary of £36,236 in Worcester and Malvern. Further, there is also a nationally recognised 'cyber dividend' with regard to salaries. Technopolis analysis indicates that in the last six months of 2017, median advertised salaries in cyber security in the region ranged from £45,000 (Tewkesbury) to £82,500 (Worcester) – with a national median of £57,000 per annum.

With regard to productivity and earnings, there is clear potential for growth in the cyber security sector to improve the region's GVA per capita, and support efforts to narrow the productivity gap over the next decade.

Further, the Audit set out to explore how the expertise within the region could be utilised to best develop talent and embed cyber resilience within firms across industries. There are strong initiatives in the region to achieve these aims, including (but not limited to) the Cyber Club, the Malvern and West of England Cyber Security clusters, and the IASME consortium[9]. Our vision for the region is to embed cyber resilience through the promotion of initiatives that encourage wider investment in cyber security products and processes across all industries.

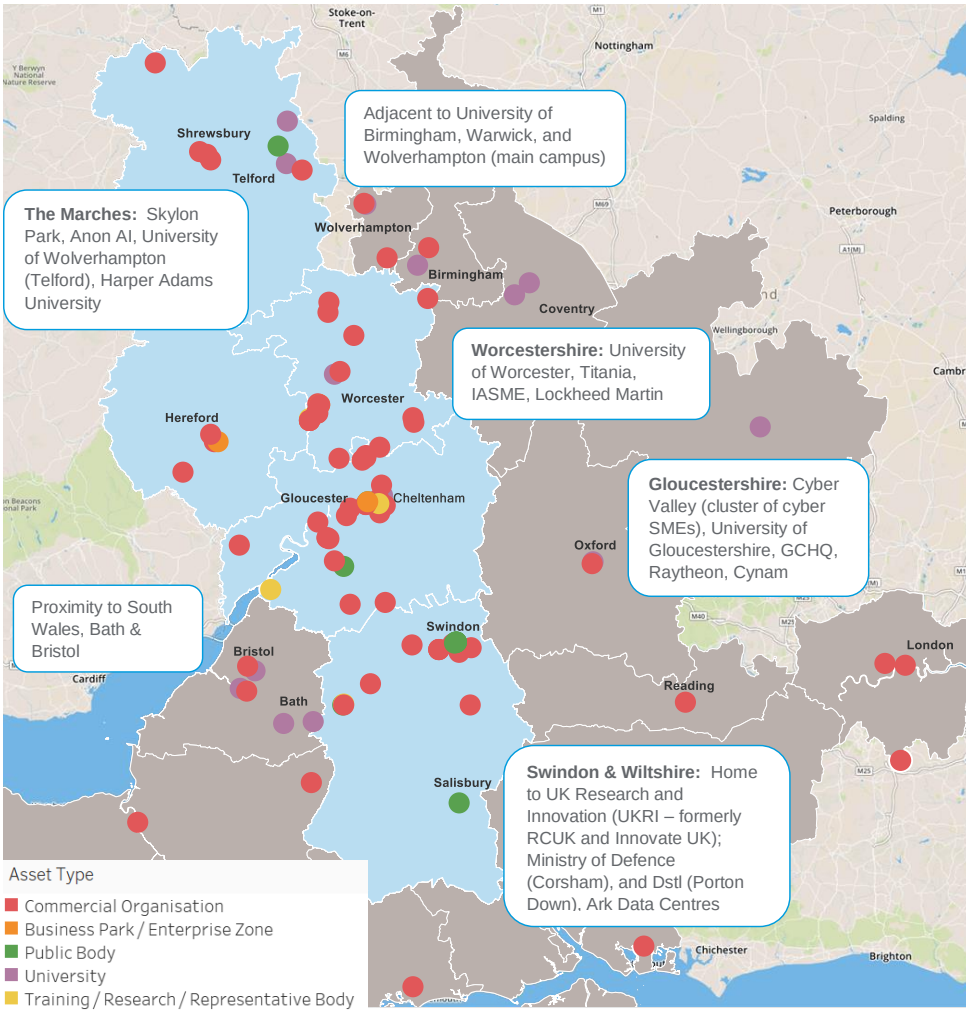
Long-term, it is our ambition that the Cyber Resilience Alliance Region is recognised as a world-leading cluster, and there are many opportunities for our businesses and organisations to embed and promote cyber resilience globally, and to lead within cyber security export markets.

[8] Business Expenditure on Research & Development. See Section 4.2 Research Strengths and 4.3 Innovation Strengths and Growth Points
[9] See Section 5.5 Local Science and Innovation Talent

Key Strengths

The Cyber Resilience Alliance region is host to strong research collaboration between government, universities, research institutions, and businesses. Despite a relatively small working age population (1.6 million), the Cyber Resilience Alliance is highly regarded with several internationally recognised cyber security clusters (Malvern, Worcester, and Cheltenham in particular).

Map of the Cyber Resilience Alliance Business, Commercial, Public, and Academic Assets:



Source: RSM, CRA Market Intelligence

The region is particularly strong in…

Research:

The SIA area has an LQ[1] of 2.2 for cyber security projects led, demonstrating that the area is twice as likely as the national average to have organisations leading publicly-funded cyber security research. This indicates that **Cyber Resilience Alliance area has above average concentrations of cyber security research.**

R&D Investment:

Within the Cyber Resilience Alliance, there is evidence that government, business, higher education institutions, and non-profit organisations are increasing expenditure in research and development. As shown in Section 4.3, nominal R&D expenditure has increased within the West Midlands and South West since 2008 at twice the rate nationally (grown 43% between 2008-14 compared to 21% across the UK).

Commercial Activity:

Within the UK itself, London is recognised as a cyber security hotspot, with more than two hundred cyber security firms estimated in the city, and many more vying for cyber security talent to support the operations and development of financial services, legal services, media and telecommunications etc.

However, the Cyber Resilience Alliance Science and Innovation Audit has enabled an overview of the firms and organisations active within the region and provides an evidence base that the region hosts the **second largest cluster of cyber security activity** outside of London.

Further, the region has a prominent defence and security community, which directly supports the growth and sustainability of the cyber sector. As a result of this community rooted in security, the region is a hotbed for cyber security innovation in the UK.

Infrastructure that supports innovation:

The region is focused upon developing its entrepreneurial and innovation support network, with emphasis on high-tech, cyber, digital and manufacturing industries. The region is home to a wide range of universities, research institutes and councils, public sector organisations, businesses, and incubation and innovation spaces active in developing the cyber security sector. This Audit has identified over a hundred assets and organisations active in supporting cyber security product and service development. Further, the region is in close proximity to several world-leading businesses, universities and research institutions active in cyber security, advanced manufacturing and automotive technologies.

Opportunities

The cyber security sector clearly presents several opportunities in the region, not just for economic growth at the sectoral level, but also through securing the crucial technological developments across wider society. Ultimately, cyber security is about embedding trust in society, economy and technology, and the Cyber Resilience Alliance region will provide the expertise to support wider transformational advancement in the UK.

There are clearly opportunities that arise from automation, Artificial Intelligence (AI) and Machine Learning, and within securing the rapid roll-out of Internet of Things (IoT) devices across the country.

Opportunities for R&D, Product Development and Enhancing Productivity:

In recent years, there has been a concerted effort on behalf of manufacturing to increase investment in research and development in the region. Given the opportunities that arise from automation, Artificial Intelligence, and machine learning for firms across the region, there are also core opportunities for the region's cyber security sector to benefit from commercial partnerships to secure these technologies.

This increased investment in transformative digital technology in the region, combined with world-leading secure solutions, will generate considerable opportunity to enhance productivity and living standards in the region.

Opportunities for Resilience:

As stated, the most recent DCMS Cyber Breaches Survey (2017) indicates that 34% of businesses have no spend on cyber security, and that four in ten experienced some form of breach last year. We will seek to further develop initiatives to tackle gaps in cyber resilience in the region e.g. funding for advice, Cyber Security vouchers, Cyber Club etc.

There is clear opportunity for the region to act as a regional testbed for initiatives that support cyber resilience to be scaled up to national level (evidence informed pilots and interventions).

Domestic and Export Growth Opportunities for the Cyber Resilience Alliance:

As identified in the UK Cyber Exports Strategy (DIT, 2018) – our region has an established, expert and innovative sector made up of companies across a full range of capabilities.

UK cyber security exports are set to grow to £2.6bn by 2021, and will be primarily driven by governments, financial services, automotive, energy and Critical National Infrastructure, healthcare and infrastructure.

Gap Analysis

Whilst the cyber security sector has demonstrated rapid expansion and growth in the region in recent years, there remain gaps that are restricting the growth and potential of the sector, and present challenges for the future sustainability and talent flow in the industry.

Within cyber security, these gaps impact not only the sector directly, but impact the UK's capacity to defend its national infrastructure and provide an adequate cyber response function regarding national security. Within the region, given the concentrated presence of cyber security businesses and critical national infrastructure, there is a fundamental need to address these gaps and to ensure a sustainable model for the growth of UK cyber security.

This audit has identified the following core gaps that must be considered in future interventions to support the sector within the region.

Development of Skills & Talent:

> **We are struggling to attract people with the correct experience and skillsets in cyber security." (**Gloucestershire SME involved in IT infrastructure security)

Several of the SME cyber security firms in the region consulted throughout this Audit process highlighted the significant gap in the region regarding a skills shortage. As reflected in Section 5.4, there are hundreds of unfilled vacancies in the region within cyber security. This is for several reasons, including:

- The **perception that the City of London has the 'pull' to attract some of the nation's best talent, leaving other parts of the UK with more limited potential for recruitment.** This highlights the need to showcase the Cyber Resilience Alliance region as attractive to live and work in;
- A **perceived gap within the skills accredited** (Level 7+) and the **applied and commercial skills required by businesses;**
- **Demand for labour considerably exceeds supply**: this is creating a labour market with salary costs potentially prohibitive to new innovative start-ups (e.g. salaries in the region of £50,000+ for staff with one to two years' experience);
- The current provision of skills and talent (formal university / higher education, and conversion courses and training schemes) offers a strong model to address many of these gaps, with the Universities of Gloucestershire, Worcester and Wolverhampton taking welcome steps to grow the talent pipeline; however, given the sector's robust growth, there is a gap between what is needed and what can be produced.

Consultees did note, however, that the Cyber Resilience Alliance region is not the only cyber security cluster vying for cyber security specialists, commenting on the need for the region to vie with talent across the entire UK.

Provision of Facilities and Infrastructure: Reflect the Breadth & Diversity of the Sector:

This Audit has identified the wide range of funding and infrastructure initiatives across the region and wider UK for cyber security. The region is host to several of the UK's leading examples of cyber security incubation and acceleration including the Wyche Innovation Centre, and the national GCHQ Cyber Accelerator programme. There are also several planned investments in cyber security infrastructure over the next few years to support sectoral growth including the Cheltenham Cyber Park, and the Marches Centre for Cyber Security. However, several consultations in the region have indicated that within the sector, investment in infrastructure has focused upon schemes supported by government and security agencies. Whilst this is welcome in growing the sector, it is viewed that there are gaps in:

- **Availability and Affordability of Grade A Office Space (all sizes):** As set out by Savills, cyber security firms are set to take up to one million sq. ft in office space across the UK by 2022. Given the demand within the sector, combined with the need for firms to ensure working space that complies with their respective standards and accreditation (ISO 27001, Cyber Essentials etc), many consultees have identified the perceived shortage of high quality office space at all levels (for small to large teams), and the prohibitive costs associated with office rental. Increasing the supply, particularly around clusters, will relieve increasing office costs, and also enable collaboration between adjacent firms – thereby supporting the region's ambition to rapidly grow the sector.

- **Provision of Product Testing and Validation Labs:** One essential process within the industry is testing products and services to provide greater assurance to consumers of the overall validity of the product being offered. As such, there are several testing labs/facilities across the UK, providing CTAS and CHECK testing accreditations which identify any weaknesses utilising publicly known vulnerabilities and common configuration faults. However, joining these schemes can be prohibitively expensive for SMEs, and take up is therefore viewed not as high as it could be with the provision of support.

NCSC has released several certified product schemes which test the validity of cyber security products and services, providing greater assurance to consumers of the reliability and effectiveness of the products they purchase, including Commercial Product Assurance, Commercial Evaluation Facilities, Commodity Information Assurance Services, Tailored Evaluation, and TEMPEST and EMS (see Appendix J).

However, some consultees argue that there is a gap that exists for an independent body to provide testing and validation labs in the region. This would enable private firms to test their products in a space that would not necessitate a standard approach i.e. sharing all relevant code or IP with a national body (see Proposal 1 – National Cyber Lab).

There is also a perceived gap that internationally – investment in UK cyber security is often conflated with London, and that the region will need to invest in a coherent vision, brand and message to promote the area as a highly attractive location for living and working.

Key Ambitions and Proposals for Growth

To best tackle the gaps within the region's cyber security sector, and to take advantage of the opportunities provided by technological transformation, this section sets out our key proposals and suggested interventions for the region.

Across the four Local Enterprise Partnerships, we estimate a financial commitment to the sector over the next five years in the region of £80m (£16m per annum)[10]

Proposal 1: Innovation, Research & Development | Investing in Infrastructure

Business Expenditure on Research and Development (BERD) within the region has been increasing in recent years, and this is arguably being driven by several large manufacturing and automotive firms within the West Midlands and South West of England. There is therefore considerable potential to utilise existing clusters and networks between these firms and innovative cyber start-ups in the region to provide commercial opportunities, and to accelerate growth.

Further, the Cyber Resilience Alliance will encourage strong utilisation of upcoming investments in cyber security infrastructure, given the expectation that such initiatives (e.g. Cheltenham Cyber Park and the Marches Centre for Cyber Security) will result in increased innovation and collaboration between newly established innovative spin-outs and start-ups.

To further enable innovation and encourage continued investment in Research and Development (R&D) in the region, the Cyber Resilience Alliance propose:

1. **Promoting Existing Infrastructure Expenditure:** The region must ensure that recent proposed investments are maintained and supported; however, these must also receive investment to join-up initiatives across the region e.g. to identify the best possible incubation space for new firms depending upon their capability, capital and ambitions. Any fragmentation of cyber security infrastructure in the region may cause a disjointed approach to seeking investment for the region**.**

2. **New Infrastructure: 'National Cyber Lab':** The Audit has confirmed the initial requirement for exploring the feasibility and potential investment in a 'new specialised data centre with a flexible cyber range and dirty lab to offer organisations the chance to engage and use these facilities in the development of cyber technology and cyber defence' which can be industry-driven.

   Given the proximity of government schemes and NCSC validation facilities, this could be scoped to become a centre of national significance e.g. a National Cyber Lab, with potential sites across the wider region – linking into wider infrastructure in the region e.g. Berkeley C11 Cyber Security Centre testing labs for University of Gloucestershire students, and the launch of UK Cloud's UKCloudX[11] service in the region (a dedicated facility which provides High Assurance cloud provision for defence and government). Membership of this centre would not only allow access to the sites but also access the subject matter experts and a

[10] See Annex A (Business Cases) for further detail and rationale.
[11] See https://ukcloudx.com/

collaborative environment where partnerships could be formed to chase the larger programmes and research funding. It would further allow access to cyber skills from the traditional industrial base. This could provide the potential for international recognition of the cluster (having industry-led testing facilities with international standards to encourage product exports). This would reflect a significant financial commitment by the region to supporting the cyber security centre.

3. **Sustained Investment in Aligned Technology:** Increased investment and adoption of innovative technologies in the region e.g. Worcestershire 5G test bed, provides regional firms with significant gains in productivity, but simultaneously requires cyber security support given the proliferation in devices and data. This provides real opportunity for sectoral growth – where the Cyber Resilience Alliance is a technological world-leader, **being a world-leader in securing these technologies is a natural extension.**

Proposal 2: Encouraging Sustainable Demand:

We will support interventions that promote the growth of the cyber security sector through domestic and export sales, and through the provision of innovative new products and technologies.

We identify the following mechanism to support this proposal:

4. **Encouraging Regional Demand**: It is the view of this Audit that the region is home to world-leading and innovative expertise. However, there remains a view by regional stakeholders that London is considered internationally as central to the UK's cyber security activity.

It is therefore crucial to provide a narrative that encourages growth at the regional level, through:

- **Highlighting the strengths, offer and capabilities of the region's cyber security expertise** through investment in suitable marketing, and schemes such as 'Meet the Buyer', Knowledge Transfer Partnerships, and sharing examples of how cyber security in the region can benefit a range of sectors e.g. agri-food, manufacturing and automotive. This could include sponsoring cyber security clusters within the region to engage with wider sectoral groups (automotive, aerospace, manufacturing, agri-food);
- Utilising the existing Local Enterprise Partnership structures to **identify opportunities to bring together cyber security firms and businesses in need of secure solutions;**
- Promoting a **marketing narrative emphasising the strengths of the region as a suitable location for cyber security investment and employment**, including space, affordable housing, high living standards, transport access and infrastructure, availability of talent, and **close proximity to bodies of national significance** in cyber security (GCHQ, MoD) and Academic Centres of Excellence in Cyber Security and active cyber security universities.

Proposal 3: Improving Skills and Talent:

For any sector to be successful, it requires a sufficient and skilled workforce. The cyber security sector has experienced considerable skills and talent shortage in recent years, and this has been reflected within remuneration levels and the extent of unfilled vacancies within the sector.

However, there is substantial demand within the sector, that can facilitate high-value employment within the region where the skills and talent are invested in sufficiently to a) increase supply of labour and b) increase the skills being requested by industry. The Cyber Resilience Alliance therefore propose to:

5. **Facilitate Workforce Planning in the Cyber Security Sector for the Region**: We propose within the Cyber Resilience Alliance to establish a working group to monitor labour supply and demand in the region to enable targeted investment and interventions. This will need to consist of regional decision-makers involved in education (across all levels), business, government and the third sector.

   Further, there is compelling evidence within the region that reskilling and lifelong learning initiatives work well in meeting labour shortages and encouraging new talent into the sector. Indeed, the region's strength in national defence and security provides cyber security as a natural career progression for many of our long-term serving personnel and provides new perspective and innovation in the sector. We will seek to encourage initiatives that encourage neurodiversity in the sector (such as the Community Cyber Operations Centre), that attract younger talent to get involved in cyber security (e.g. Cyber Schools Programme), and those schemes that seek to move people away from potential cyber-crime into security roles.

6. The Cyber Resilience Alliance is a prime location for innovative approaches in encouraging new talent into the sector, and **we will monitor and seek to support funding requirements accordingly given the potential for significant increases in regional productivity as a result of increased sectoral employment**.

7. Finally, the Cyber Resilience Alliance is home to several university accredited courses in cyber security. There are also several universities adjacent to the region that offer courses in cyber security including University of Warwick, University of Birmingham, University of Bristol, Bath Spa, and University of South Wales – demonstrating the importance of neighbouring institutions. There has been considerable growth and interest in cyber security courses in the region. **We propose that the region has potential to become home to one of the UK's first 'Centres of Excellence in Education within Cyber Security',** similar to the EPSRC accredited Academic Centres of Excellence in Cyber Security Research (or the National Security Agency (NSA) /Department of Homeland Security (DHS) Centers of Academic Excellence in Cyber Defence program[12]) - which receive international acclaim, yet focus on how to teach cyber security in an applied format of benefit to employers in the region such as Raytheon, BT, Lockheed Martin and QinetiQ and support 'life-long learning' in the region.

[12] https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

Proposal 4: Focused Marketing & Sector Targeting:

The Audit has also validated that cyber security clusters work where there is a clear awareness of the anchor-driven strengths to encourage talent and investment to flow into the region. Within the Cyber Resilience Alliance, there is national and international recognition that cyber security activity is strong; however, there is a risk that this can become disjointed through recognition of several smaller clusters contained within e.g. Malvern, Gloucestershire, Cheltenham, and Wiltshire etc. Indeed, the geography of the region can also often mean that the West Midlands and South West can be assumed to mean 'Birmingham' and 'Bristol' respectively; which presents a challenge to the region regarding being known on the map.

This evidences the need for the Cyber Resilience Alliance to establish a unified consortium, brand and approach to attract investment and talent.

We propose to:

8. **Sustain a Cyber Resilience Alliance representative body,** combining representation from each of the four Local Enterprise Partnerships (government, business and academia), to promote the sector. The management and governance of this body could be agreed in consultation with local, regional, and national government bodies.
9. **Establish a Cyber Resilience Alliance website / dedicated support** to demonstrate how a start-up / SME / large multinational can do business in the region (e.g. access to space, labour, grants and loans, R&D tax credits, university / research support) to ensure coherency;
10. **Establish formal Cluster Partnerships,** potentially 'twinning' the Cyber Resilience Region with comparable initiatives in the United States or other countries with prominent or emergent sectors (e.g. Israel, China, or Brazil);
11. **Marketing:** Promote the region as a high-growth location with a growing and talented labour supply, with support from LEPs to invest, start and grow – where firms will be surrounded by other world-leading innovative firms and public bodies (drawing upon the Midlands Engine Cyber momentum).
12. **Intelligent sectoral targeting:** The Cyber Resilience Alliance will identify and track firms active in sectors aligned to the four LEPs growth priorities (manufacturing, agri-food, professional services) in addition to export potential (Government, Financial Services, Energy and CNI, Healthcare, and Infrastructure), and will identify their respective approach to cyber security (spending, research, relationships with regional suppliers etc.).
13. **Enhancing Opportunities for Investment:** We will explore opportunities to bring more events, and conferences (and specialist VC investors) to the region to showcase the talent and expertise of the region.

Networking and Collaboration

The consortium delivering this audit brings together a wide range of academic, research, innovation and commercial strengths in the fields of cyber security and economic development.

It is led by Worcestershire Local Enterprise Partnership with support from Gloucestershire, Swindon & Wiltshire and The Marches LEPs, and has focused on the needs of the research and business community within cyber secuity, through concentrating on the economic impact, exploitation, and investment potential of cyber capabilities and capacity across the region, while taking cognisance of academic teaching, and IP generation as underpinning elements.

Throughout this process, the Science and Innovation Audit received written or verbal evidence from over sixty leading members of business, academic and public bodies. These contributions are greatly appreciated by the Cyber Resilience Alliance, and have been an valuable call to action for the region.

The Cyber Resilience Alliance have also utilised this exercise to promote collaborative and joint-up initiatives across the region in cyber security and beyond. This includes:

- The Cyber Valley marketing initiative being supported by the Midlands Engine Cyber necessitating close co-operation between Skylon Park, Marches LEP, and Worcestershire LEP who have been leading the initiative. This also means that the trade partnership within Cyber Maryland are aware of the Cyber Resilience Alliance concept, and collaboration being undertaken to grow the region;
- Cheltenham will host the National Cyber Awards 2018 in November, supported by the Cyber Trust, Cyber Security Challenge, and GFirst LEP. This event rewards those who are committed to cyber innovation, cyber crime reduction and protecting the citizen online, and has been supported through relationships developed as a result of this SIA.
- The four Local Enterprise Partnerships involved within this exercise are committed to work collaboratively to identify, share and learn from interventions and infrastructure investment in the region. This means sharing ideas, innovation and working space to give companies in the region the best opportunities to grow.

Further, the Cyber Resilience Alliance will work as closely as possible with other SIA regions to identify opportunities to grow the wider UK cyber security sector. It is considered that this SIA is particulary complementary to the Midlands Engine SIA (Wave 1), Innovation South (Wave 2), Oxfordshire Transformative Technologies (Wave 2), and Applied Digital Technologies, South Wales Crucible, and Upstream Space SIAs (Wave 3).

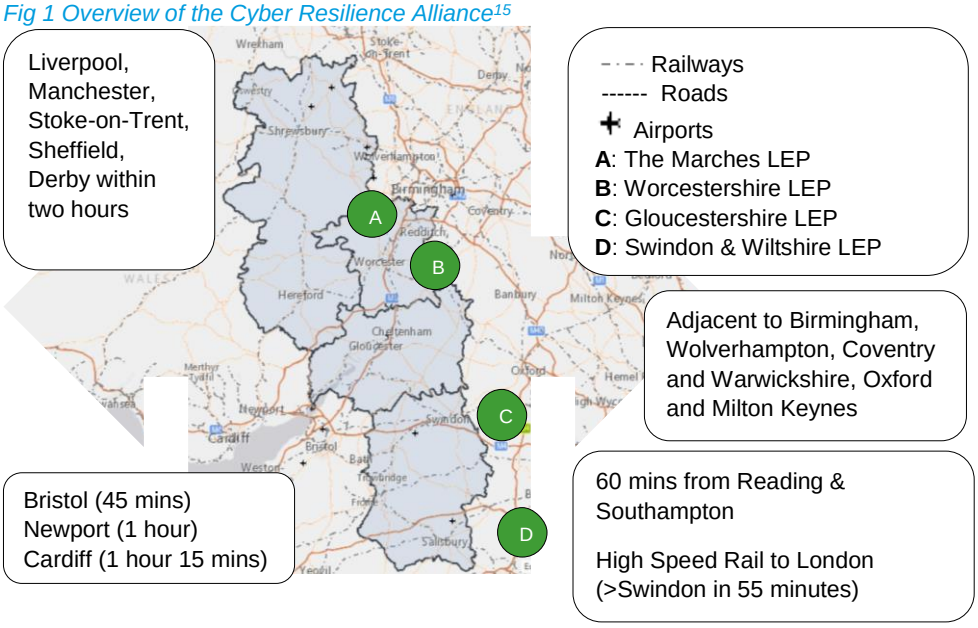
3. INTRODUCTION TO THE SIA REGION

3.1 SIA Geography and Specialisation

The Cyber Resilience Alliance region consists of four Local Enterprise Partnerships (LEPs)[13], stretching from north of Shrewsbury to south of Salisbury (over 180 miles). The region spans more than 5,200 square miles (10.4% of England's total geography), with 2.59 million residents, of which 1.58m are aged between 16-64[14] (3.8% of the UK's working age population).

At its heart, it includes the urban settlements of Worcester, Cheltenham, Gloucester, Hereford, Telford, Swindon and Shrewsbury which are well-connected to the rest of the country via strong high-speed rail links and the M4 corridor (connecting South Wales, Bristol, Swindon, Reading and London) and the M5 motorway corridor that runs from Birmingham through to Bristol (through the centre of Worcestershire and Gloucestershire LEPs). The region is synonymous with UK defence and security and is home to some of the world's largest defence firms (BAE Systems Applied Intelligence in Gloucester, Babcock in Swindon, and Lockheed Martin in Wiltshire), as well as the UK's highest levels of public security (Ministry of Defence in Corsham, and GCHQ Cheltenham).

Fig 1 Overview of the Cyber Resilience Alliance[15]



[13] (The Marches, Worcestershire, Gloucestershire, and Swindon & Wiltshire)
[14] ONS Population Count (Estimate, 2016). Available at https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland
[15] Produced by RSM, Source: ESRI, Garmin, Office for National Statistics.

3.1.1 The Economy

- The Cyber Resilience Alliance is a £58.6bn economy, generating 3.55% of the UK's Gross Value Added (GVA)[16].
- There are 95,660 active firms in the Cyber Resilience Alliance region. (37.2 businesses per 1,000 population).[17] On average, each business in the region has 11 employees.
- 99.7% of businesses in the region are SMEs. (89.8% micro, 8.4% small, 1.5% medium, 0.3% large).

The region's leading industries include:

Industry	*CRA GVA (£m)*	*Proportion of CRA's GVA*	*Contribution to UK Sector (% GVA)*
Agriculture, Forestry and Fishing	984	1.7%	8.0%
Manufacturing	9,293	15.9%	4.8%
Production (other than manufacturing)	1,945	3.3%	4.2%
Real Estate Activities	8,502	14.5%	4.0%
Construction	3,610	6.2%	3.5%
Other Services and Household Activities	2,197	3.8%	3.5%
Public Administration, Education & Health	10,606	18.1%	3.5%
Distribution, Transport, Accommodation and Food	10,676	18.2%	3.5%
Business Service Activities	5,356	9.1%	2.9%
Information and Communication	2,643	4.5%	2.5%
Financial and Insurance Activities	2,777	4.7%	2.3%
Total	**58,591m**	**100%**	**3.55%**

These industries can all benefit from reduction in disruption or loss that can come through the securing of digital assets. The growth of the cyber security sector in the Cyber Resilience Alliance region will therefore be crucial for UK economic performance, and matters of national security.

[16] Data compiled by Technopolis based on ONS Regional GVA(I) by local authority in the UK (March 2017) Available at: https:///www.ons.gov.uk/economy/grossvalueaddedgva/datasets/regionalgvaibylocalauthorityintheuk
[17] Data compiled by Technopolis based on ONS Business Demography (November 2017). Available at: https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/datasets/businessdemographyreferencetable / Comparison: There are 2,405,980 firms in the UK (36.95 per 1,000 pop).

Securing the UK's Critical National Infrastructure (CNI):

- CNI consists of nine key sectors for the smooth running of the UK's society and economy (energy, food, water, transportation, communications, emergency services, health care, financial services, and government). These sectors directly provide over 30% of the region's GVA, and indirectly support the wider economy. Within the Cyber Resilience Alliance region, the agri-food sector (The Marches), and financial services (Swindon and Wiltshire) sectors are particularly in need of secure solutions.

- Cyber security is at the heart of securing critical national infrastructure, and the National Cyber Security Centre (headquartered in London) and GCHQ (Cheltenham) provide protective security advice to key infrastructure businesses, therefore minimising the UK's risk and vulnerability to terrorism, espionage and national security threats.[18]

Advanced Manufacturing: The Cyber Resilience Alliance is home to one of the UK's largest manufacturing clusters (£9.3bn Gross Value Added, which reflects 5.5% of the UK's manufacturing GVA despite having 3.8% of the population)[19].

Cyber Security Vendors in a Resilient Economy: The Cyber Resilience Alliance is home to some of the UK's most innovative start-ups and growing firms in cyber security, including Cheltenham's GCHQ Cyber Accelerator. As UK cyber security firms grow, their capacity to innovate and provide products and services to UK firms also expands, which supports making the UK (and the Cyber Resilience Alliance region) one of the safest countries in the world to do business in the digital economy.

3.1.2 Location Quotient Mapping

- Location Quotient (LQ) analysis demonstrates areas of specialisation with a region. It compares the area's business count and employment data to the national average (e.g. where the region has 15% of its population employed in a particular sector compared to 10% across the UK, this provides a LQ of 1.5. Any LQ >1.0 indicates a higher proportion of employment or businesses than would be expected at national level.
- This analysis for the Cyber Resilience Alliance region indicates strengths in **Manufacturing** with over 7,000 local units and almost 130,000 employed – (LQ-E 1.46, LQ-LU, 1.15), **Public Administration and Defence (**44,900 employed, and 1,235 local units), and **Wholesale and Retail** (187,500 employed with 21,000 local units).
- Whilst employment and business count data for '**Information and Communication'** (which typically includes IT and software development roles) may be lower than the national picture

[18] Cabinet Office, *Public Summary of Sector Security and Resilience Plans*. 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf

[19] Data compiled by Technopolis based on ONS Regional GVA(I) by local authority in the UK (March 2017) Available at: https:///www.ons.gov.uk/economy/grossvalueaddedgva/datasets/regionalgvaibylocalauthorityintheuk

(employment of 34,200 – LQ 0.76, and local unit count 8,300 – LQ 0.89), there is still a considerable volume of business activity which can enable the scale-up of cyber resilience in the regional economy. The Cyber Resilience Alliance region is therefore well placed to take advantage of the six most promising sectors for cyber security exports and growth worldwide (**Source**: **DIT UK Cyber Security Export Strategy, 2018[20]):**

1. **Government**: (£27.6bn) : Government spending on cyber security is being driven by global and growing awareness of the threats posed by inadequate security in the context of digital transformation in government and public sector organisations.

2. **Financial Services**: (£16.1bn): Consumer trust is vital to the financial services industry, and the UK is a global leader in financial services and FinTech. Within the Cyber Resilience Region, securing financial services is a vital function; particularly in Swindon where Nationwide Building Society Headquarters is a major recruiter for cyber security talent.

3. **Automotive**: (£0.9bn): The emergence of autonomous vehicle and real-time traffic and vehicle management information systems provides real security implications and challenges. Vehicles will ultimately be networked, and reliant upon secure systems to minimise risk of collision.

4. **Energy & Critical National Infrastructure**: (£0.8bn): Digital infrastructure is increasing at scale, including the rapid emergence of smart grids and devices which may cause vulnerabilities for the sector. Further, CNI consists of a large number of legacy systems (often dating back over twenty years) which require ongoing maintenance to ensure sustainable security.

5. **Healthcare** (£4.1bn): Healthcare delivery services and pharmaceutical companies have large quantities of patient data and valuable intellectual property to protect.

6. **Infrastructure**: (£0.7bn): As with other sectors, improvements to consumer and delivery infrastructure (e.g. smart tickets, airport scanners etc.) provide potential for severe disruption or loss of personal data if systems are compromised.

[20] Figures shown in brackets refer to global spending (in cyber security) estimates in 2016

Fig 2. Location Quotient Analysis of the Cyber Resilience Alliance

Fig. 2 demonstrates the proportional strength (measured by number of firms and people employed) of the **Manufacturing** and **Public Administration and Defence** sectors in the region.

Source: Data compiled by Technopolis based on NOMIS official labour market statistics, Business Register and Employment Survey (BRES, open access version) and UK Business Counts – Local Units (September 2017) – Available at *www.nomisweb.co.uk*

3.1.3 Productivity & Earnings

Median annual (gross full-time) earnings with the region are £24,082. This is more than £4,000 lower than the national median (£28,213). However, median earnings do outperform the national median in Swindon, Gloucester, and Tewkesbury.

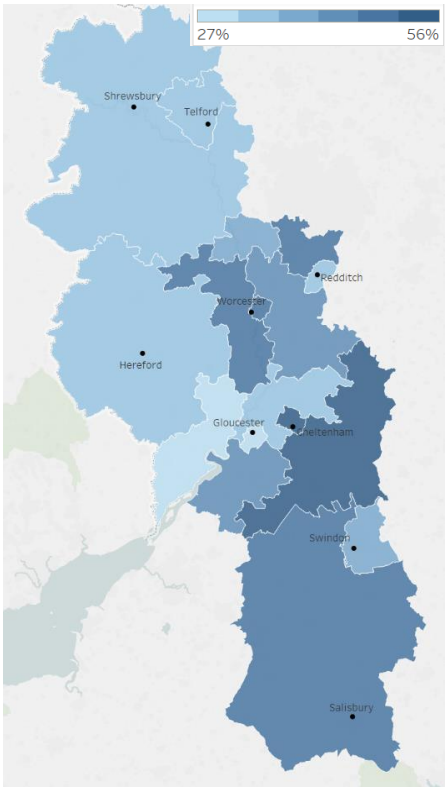
GVA per capita in the region is £22,804 (2015)[21]. This means that productivity is 10% lower than the UK's GVA per capita (£25,351). However, the region varies by local authority region, with Swindon (£30,771), Tewkesbury (£30,346), Cotswold (£29,214), Cheltenham (£27,757) and Gloucester (£26,912) outstripping the UK average; and Malvern Hills (£18,968), Forest of Dean (£16,859), and Wyre Forest (£15,783) lagging in economic productivity.

[21] Data compiled by Technopolis based on ONS Regional GVA(I) by local authority in the UK (March 2017). Available at: https://www.ons.gov.uk/economy/grossvalueadded/datasets/regionalgvaibylocalauthorityintheuk

3.1.4 Our People

The region spans more than 5,200 square miles (10.4% of England's total geography), with 2.59 million residents, of which 1.58m are aged between 16-64[22] (3.8% of the UK's working age population).

Fig. 3 Percentage of Population with NVQ4+



The standard of education is good within the region (see Fig 3).. More than two-in-five (40.65%) of the working population hold a NVQ4 qualification or above, and a further 18.96% hold an NVQ3. This compares to 43.2% with an NVQ4+ in England overall.

Cheltenham (55.6%), Cotswold (54.9%), Malvern Hills (49.8%), and Worcester (48.3%) are particularly well qualified (NVQ4+) with a qualification gap in Gloucester (26.8%), Forest of Dean (31.3%), and Tewkesbury (33.1%).[23]

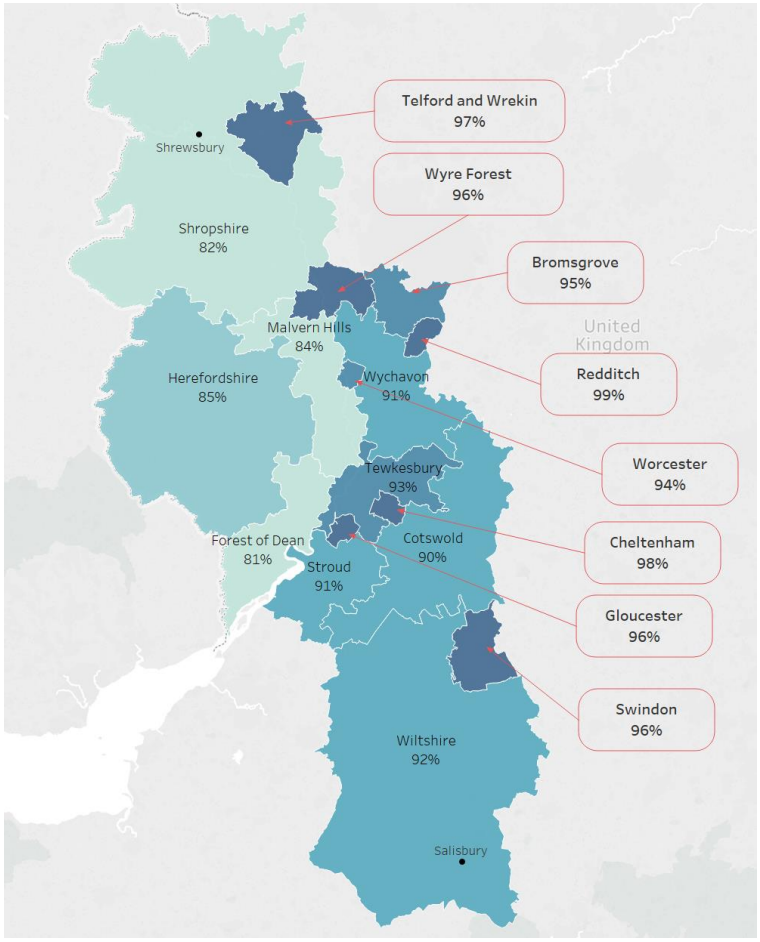
The percentage of those employed in Science, Research, Engineering and Technology related professions (SOC21) is similar within the Cyber Resilience Region (5.74%) compared to the rest of England (5.6%). However, it is noticeably higher within Stroud (11.2%), Cheltenham (9.9%), Bromsgrove (8.8%), Malvern (8.4%), Tewkesbury (8%), and Swindon (7.7%).

[22] ONS Population Count (Estimate, 2016) // Data Compiled by Technopolis based on NOMIS official labour market statistics, population estimates – local authority based by age band (Sept 2017). Available at http://www.nomisweb.co.uk

[23] Data compiled by Technopolis based on NOMIS official labour market statistics, Annual Population Survey (Sept 2017), available at http://www.nomisweb.co.uk

3.1.5 Broadband Coverage:

Fig 4. Percentage of Population with Access to Superfast Broadband (over 30MBps)



Source; thinkbroadband.com

95.3% of England's broadband coverage is considered superfast, which is over 30MBps (04/2018). This is compared with 96.2% for the SIA region, demonstrating relatively strong digital infrastructure. Worcestershire has superfast broadband coverage of 94.1%, Gloucestershire (92.1%), Shropshire (81.9%), Herefordshire (85.4%), Telford and Wrekin (96.7%), Swindon (96.3%), Wiltshire (91.8%).

3.2 SIA Hypotheses

The UK's National Cyber Security Strategy (2016-21) sets out an ambitious vision for the UK to be a world leader in cyber by 2021. The strategy concentrates on building on UK capability and developing the skills needed by exploiting the country's talent pool.

One of the main conclusions that can be drawn from the Strategy is that UK and regional prosperity will rely on **building a cyber-resilient ecosystem** to deliver increased value across all sectors including manufacturing, agri-food, and professional services etc. through best exploiting innovations such as the Internet of Things (IoT) in a 'secure-by-design' approach.

Within the Cyber Resilience Alliance region, we recognise the considerable **concentration of cyber skills within the population, largely due to proximity to GCHQ which in recent years has also encouraged a wide range of start-ups through the Cyber Accelerator, as well as encourage investment from cyber security organisations.** This means that a number of our firms are also innovative and developing industry-focused cutting-edge cyber security products.

The key to industrial success in the future is not just establishing cyber businesses. It is also about embedding cyber skills into the existing industrial infrastructure providing competitive advantage and increasing opportunities for employees to develop skills that make them and their business more attractive on a global market. We also recognise that skills being currently developed could be vulnerable to future automation with a need to ensure there is a route to maximise high value skills and increase resilience moving forward.

2. There is a strong **concentration of skills in cyber security within the region, which can be used to embed cyber resilience through a wider industrial base,** including making a strong contribution to the growth of the UK's cyber security sector directly, and supporting industries within which their demand for secure solutions will incubate, support and grow the region's economy.

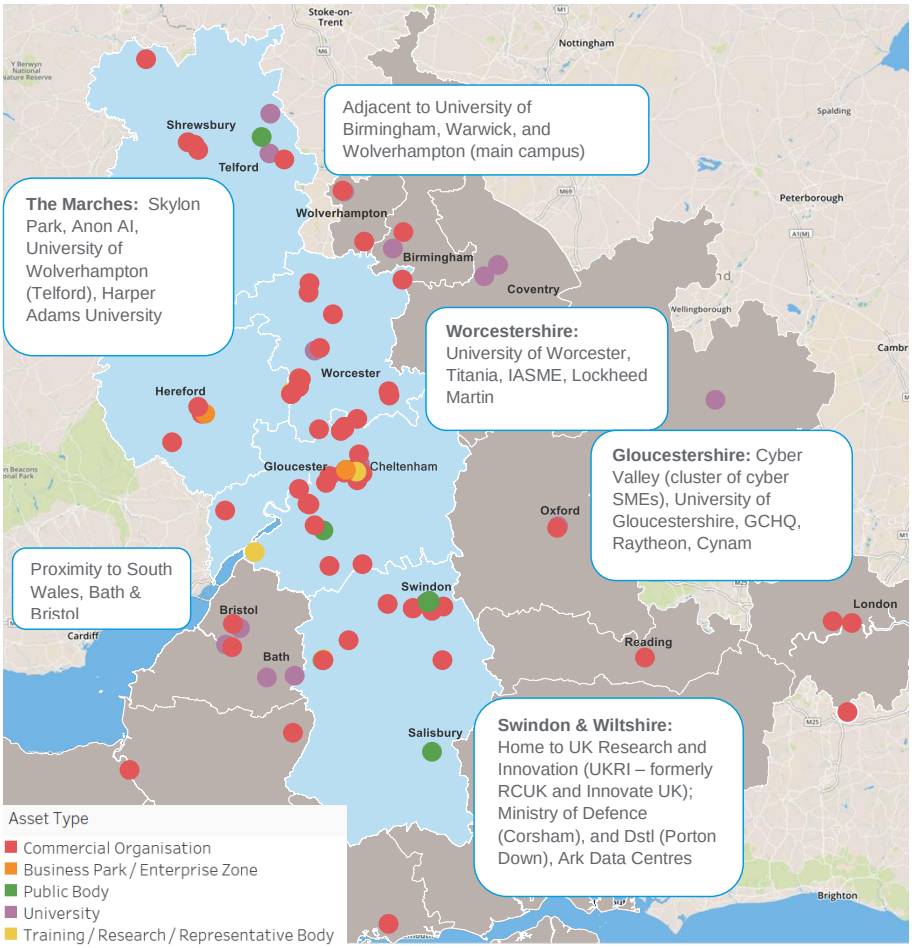
2. **Sustainable business needs to be competitive and trusted. Do traditional businesses do enough to understand and embrace cyber resilience, and how can they best invest accordingly?**

The Audit will identify opportunities to build linkages between the strong regional cyber security expertise and the wider community.

3.3 Overview of SIA Geography

The Cyber Resilience Alliance region is host to strong research collaboration between government, universities, research institutions, and businesses. Despite a relatively small working age population (1.6 million), the Cyber Resilience Alliance is highly regarded with a number of internationally recognised cyber security clusters (Malvern, Worcester, and Cheltenham in particular).

Fig. 5: Map of Cyber Resilience Alliance Assets



Source: RSM / CRA Market Intelligence

3.4 Research Strengths

The Cyber Resilience Alliance is home to several universities, businesses and public organisations active in cyber security research across the UK and internationally. This section evidences the research base active within the region.

3.4.1 Research activity

The following tables provide analysis of publicly-funded research and innovation activity in cyber security over the period 2007 to 2017. For comparative purposes, the tables also summarise the situation for publicly funded research in the related area of 'data science.' Location quotients[24] (LQs) provide a way of show whether the partnership area has a higher concentration of research activity relative to the UK average. In short, a LQ of 1 indicates that research activity under a topic is as heavily concentrated in the partnership area as it is across the comparator geography overall (the UK in this case). **A LQ greater than 1 signals a level of activity/specialisation that exceeds what would normally be expected nationally while below 1 indicates a lower concentration relative to the national average.**

Table 1: Cyber Resilience Alliance-based organisations as project leads for publicly-funded research projects

	Projects led from the SIA	*% of UK projects*	*LQ*	*Value of projects led from SIA (£m)*	*% of UK funding*	*LQ*
Cyber Security	23	2.06%	**2.22**	£1.6m	0.39%	**0.40**
Data Science	36	0.54%	**0.58**	£9m	0.30%	**0.31**
All topics	**621**	**0.93%**	**--**	**£284m**	**0.98%**	**--**

Table 2: Cyber Resilience Alliance-based organisations as project participants for publicly-funded research projects

	Projects with participants from the SIA	*% of UK projects*	*LQ*	*Value of projects with participants from the SIA (£m)*	*% of UK funding*	*LQ*
Cyber Security	84	7.53%	**1.26**	£62m	14.81%	**1.16**
Data Science	537	8.08%	**1.35**	£523m	17.39%	**1.36**
All topics	**4,009**	**6%**		**£3.7bn**	**12.78%**	

Source: Technopolis Group, using Gateway for Research data and semantic text analysis powered by SpazioDati

[24] A more detailed explanation on how we derive LQs is provided in Appendix I. It should be noted that more narrowly defined topics can display LQ values that are more volatile, so comparison across topics should not be taken literally.

As shown, **organisations in the Cyber Resilience Alliance area led just over 2% of all the UK's cyber security research projects**, while the area also provided **participants to 7.5% of the UK's cyber security projects.**

The LQs both for projects led and projects participated in **indicate a high concentration of cyber security research activity in comparison to the UK.**

The SIA area has an LQ of 2.2 for cyber security projects led, demonstrating that the area is twice as likely than the national average to have organisations leading publicly-funded cyber security research. The LQ is also substantially higher than the SIA area's LQ for data science projects led (0.58). Although the SIA area's LQ for project participants is not as high as for projects led (1.26 against 2.2), it still indicates that **Cyber Resilience Alliance area has above average concentrations of cyber security research.**

The tables also show the position of SIA-based organisations with respect to the funding received for cyber security research. *Table* 2 shows SIA-based organisations received nearly 15% of the total research funding provided to cyber security projects. **This share is higher than might typically be expected (relative to the national average), as shown by the corresponding LQ of 1.16, and further demonstrates how the Cyber Resilience Alliance has an above average concentration of cyber security research.**

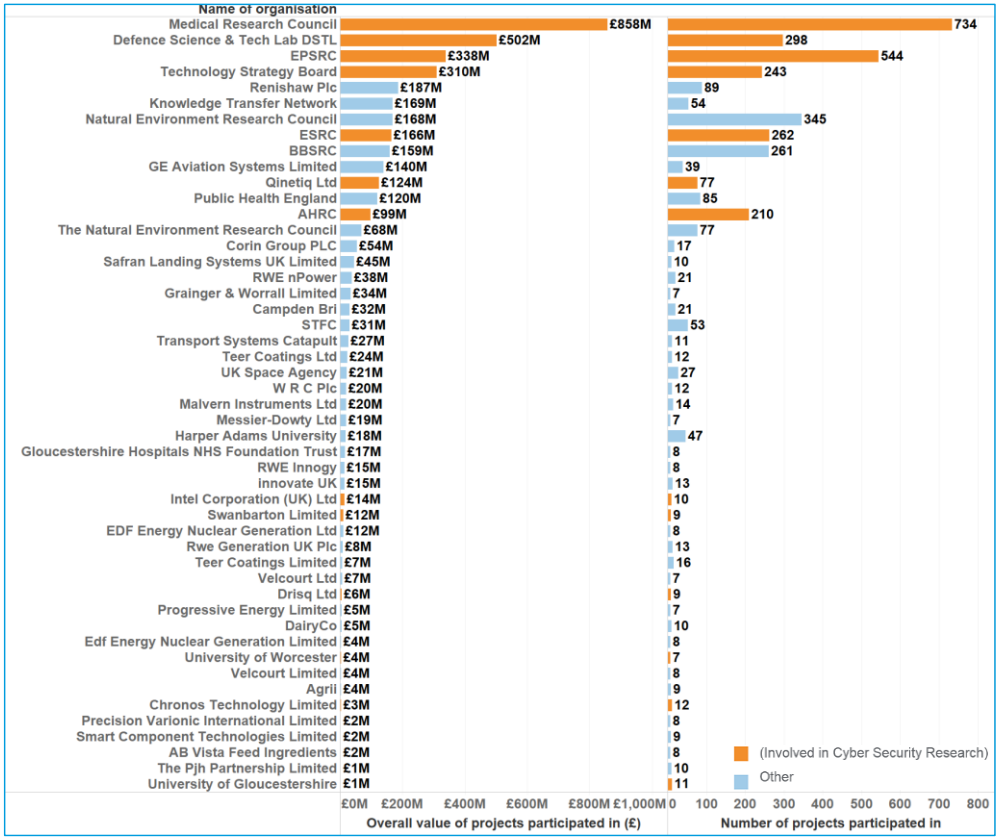
The SIA area appears to be less strong in commanding funding when the lead organisation in cyber security projects. *Table 1* shows that of all funding given to leads of cyber security research projects, organisations, SIA-based organisations only accounted for 0.39%. Indeed, this share is much lower than might typically be expected at a national level, as shown by the corresponding LQ of 0.4. These low figures are most likely caused by the absence of research-intensive universities in the SIA region.

Many of the larger grants appearing in Gateway to Research are UK research council-funded and will typically be led by the research-intensive universities absent in the partnership area. SIA area-led projects appearing in Gateway to Research are therefore most likely to be much smaller Innovate UK awards and as such, account for a much smaller share of the overall funding pot. This is not indicative of the SIA-region having below-average activity levels in cyber security research, after all, it has an LQ of 1.16 in cyber security project participants. Instead, the low figures merely reflect quirks in the data.

The following tables show the organisations in the Cyber Resilience Alliance area that have most frequently been involved in publicly funded research between 2007 and 2017. Duplicates may exist where organisations have bid under different names (which is sometimes the case where an organisation uses different subsidiaries to bid for public funding).

All topics:
Fig 6 below shows the 50 SIA-based organisations with the most project participations across all research topics. As shown, research councils play a particularly prominent role. Together, the Medical Research Council, EPSRC and the Natural Environment Research Council account for 34% of the research projects participated in by SIA-based organisations. Furthermore, three other research councils (ESRC, BBSRC and AHRC) are amongst the ten most frequent participants in research projects.

Fig 6. 50 SIA-based organisations with the most project participations across all research topics



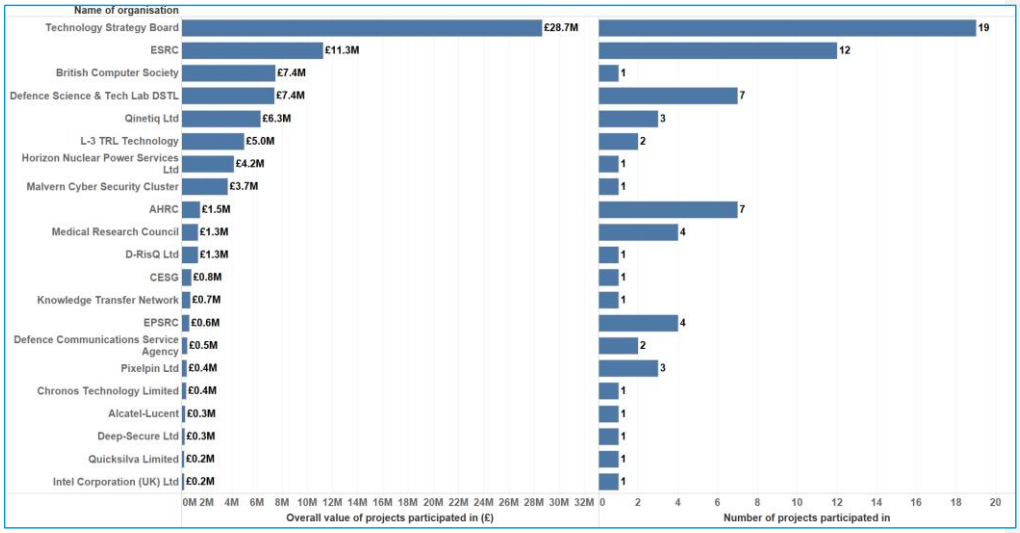
Source: Technopolis analysis of Gateway to Research data

The defence sector also accounts for fair share of project participations with Dstl and QinetiQ also being amongst the ten most frequent research project participants. Together they accounted for 8% of all the SIA area's project participations.

Cyber security

As shown in Fig 7, funding bodies account for many of the cyber security project participations by organisations based in the SIA area. Taken together, the Technology Strategy Board (now Innovate UK), ESRC, AHRC, EPSRC, and Medical Research Council accounted for nearly half (48%) of all project participations in cyber security. Only three private organisations were involved in more than one publicly-funded cyber security projects: QinetiQ, PixelPin, and L-3 TRL.

Fig 7 Cyber Security Research Projects (Organisations by value and number)



Source: Technopolis analysis of Gateway to Research data

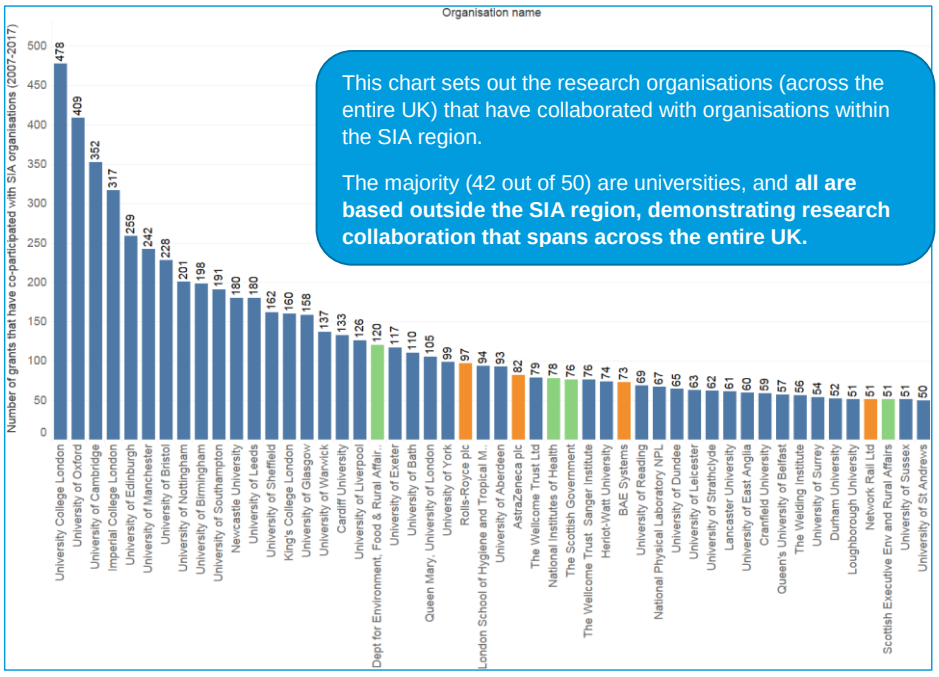
3.4.2 Organisations collaborating with SIA-based research outfits

Analysing the organisations that participated in funded projects with Cyber Resilience Alliance-based researchers will help reveal more about the SIA area's reach, including with research-intensive institutions in neighbouring areas. The following figures show the organisations that most regularly collaborated with SIA-based outfits over the period 2007 to 2017.

All topics

The figure below demonstrates research organisations that collaborate with SIA based research outfits across all topics. The list is dominated by higher education institutes with 19 organisations ranked 1-20 being universities. UCL, Imperial, Oxford and Cambridge, all institutions located within UK's so-called 'Golden Triangle' of science and technology, account for 7% of all collaborations. The SIA area's reach has also extended much further north with institutions like universities of Edinburgh and Manchester being amongst the most frequent co-participants.

Fig 8. The 50 organisations to have most frequently collaborated with SIA-based organisations – across all topics

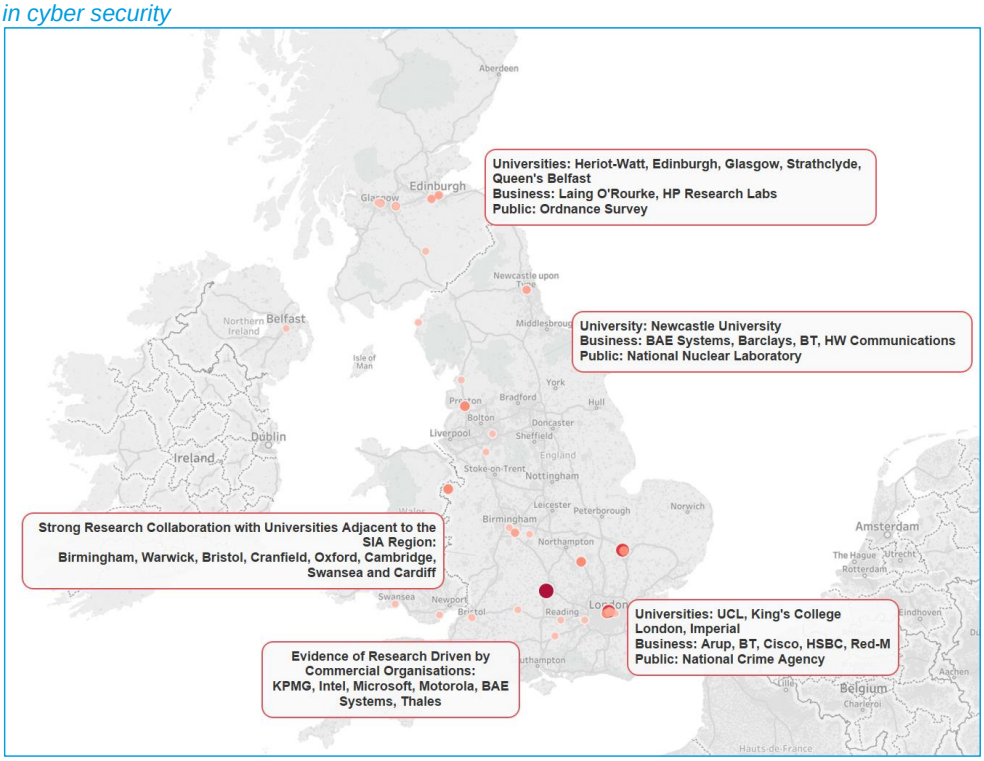


Source: Technopolis analysis of Gateway to Research data

Cyber security

As Figure 9 shows, relatively few organisations had multiple collaborations with SIA-based researchers when it came to cyber security projects. Indeed, only 16 organisations had more than two co-participations with those based in the Cyber Resilience Alliance area. Again, universities were amongst the most frequent collaborators. Four (Oxford, Cambridge, UCL and Imperial) accounted for 8% of all collaborations with SIA-based organisations. In terms of private firms collaborating with the SIA area, Microsoft, BAE Systems and BT were all amongst the top ten co-participants. The three operate in different sectors (albeit that some operations may have some overlap), showing the cross-sectoral reach that the SIA area's cyber security organisations have in research projects.

Fig 9. The 50 organisations to have most frequently collaborated with SIA-based organisations – in cyber security



Source: Technopolis analysis of Gateway to Research data

3.4.3 Examples of Cyber Security Projects in the SIA:

Whilst the Gateway to Research data demonstrates that cyber security research is active in the region, the examples below provide further context regarding the strengths of the region, and how research can be translated into successful commercial outcomes.

QinetiQ (Led by University College London): 'Exploiting interference for physical layer security in 5G Networks [CI-PHY] (EPSRC-FNR)[1] (Feb 2018 – Jan 21, Funded by EPSRC, £626,095): Project Summary and Partners:

Physical layer security (PS) provides an extra layer of security on top of the traditional cryptographic measures. It obstructs access to the wireless traffic itself, thus averting any higher layer attack. Encompassing a number of key technologies spanning secure beamforming, artificial noise design, network coding, cooperative jamming, graph theory, and directional modulation, PS is now commonly accepted as one of the most effective forms of security.

While appealing as a theoretical concept, PS still faces a number of critical challenges that prevent it from wide commercial adoption in 5G and beyond, involving the lack of secure 5G signalling, the provision of eavesdroppers' information, and the applicability of existing theoretical techniques in real environments and under low-specification hardware.

CI-PHY addresses the above mentioned challenges and promotes a paradigm shift on security by exploiting interference. In particular, CI-PHY exploits constructive interference for Physical Layer Security by:

- Specifically tailored fundamental waveform design to exploit interference, that provides a low complexity solution with limited hardware requirements;
- Artificial noise and jamming to actively improve the desired receivers' SNR under secrecy constraints, and further improve secrecy by designing the artificial noise to align destructively to the signal at the eavesdropper;
- Robust approaches for real implementation by taking hardware impairments into account to reduce the hardware requirements for providing secrecy with resource-constrained devices;
- Real implementation and over-the-air testing of security solutions to evaluate and optimise performance in commercially relevant environments.

CI-PHY will be performed with the Interdisciplinary Centre for Security, Reliability and Trust in University of Luxembourg, and industrial partners **QinetiQ, BT, National Instruments and Huawei**, and aspires to kick-start an innovative ecosystem for high-impact players among the infrastructure and service providers of ICT to develop and commercialize a new generation of secure and power-efficient communication networks, and address the unprecedented vulnerability of emerging ICT services to cyber threats**.**

PixelPin, **Supported by Innovate UK (£249,256 – Jan – Dec 2016):** In 2014, the cost of online password breaches was around $200Bn, demonstrating clearly that current solutions which centre predominantly on alphanumeric passwords are falling short of properly protecting personal and financial information.

PixelPin aim to address the limitations of current authentication solutions through the development of a secure single sign-on solution that eliminates traditional alphanumeric passwords (can also be used as part of a multi-factor approach).

The concept instead is a patented picture-based approach with users choosing a personal image (e.g. a holiday photo) and a four pass-point sequence which, based on successful PoC studies, have shown to be easier to learn, quicker to enter & less likely to be forgotten, protecting against common hacking techniques such as dictionary attacks, social engineering, phishing & keylogging. This cloud-based service allows the user to input their four pass points on mobiles, tablets or the web.

PixelPin is designed for today's always-on, mobile-first and multi-device generation. It replaces password and PINs with a secure, user friendly and private method of logging into web sites, providing a global solution that is language independent and perfect for mobile.

Project: A number of critical usability features must be developed throughout the 12-month project which will advance the technology into a preproduction prototype prior to product launch in the authentication software market in Q2 2017.

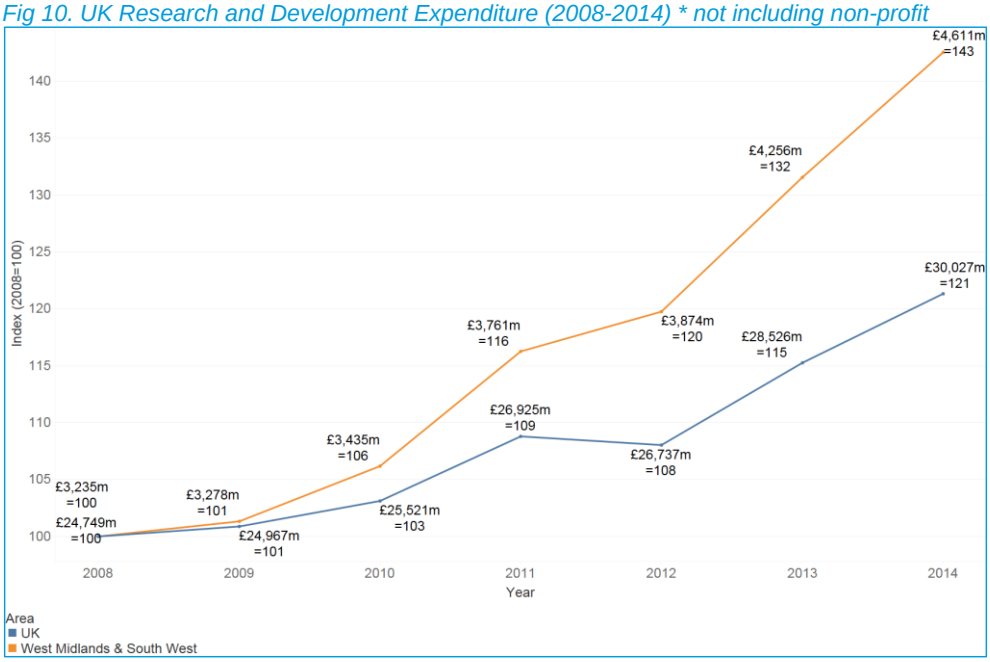
3.5 Innovation Strengths and Growth Points

3.5.1 Government and Business Expenditure on Research & Development:

The UK's Industrial Strategy sets out clearly that the government and private sector must invest more in research and development[25] to improve national productivity, and to maintain the UK's position as a global leader in science and innovation. Within the Cyber Resilience Alliance, there is evidence that government, business, higher education institutions, and non-profit organisations are increasing expenditure in research and development.

As shown in Figure 10 below, **nominal R&D expenditure has increased within the West Midlands and South West[26] since 2008 at twice the rate nationally** (grown 43% between 2008-14 compared to 21% across the UK).

*Fig 10. UK Research and Development Expenditure (2008-2014) * not including non-profit*



Source[27]: ONS BERD (2016)

[25] The Industrial Strategy White Paper sets out a policy to raise total UK R&D investment to 2.4% of GDP by 2027. (Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf)

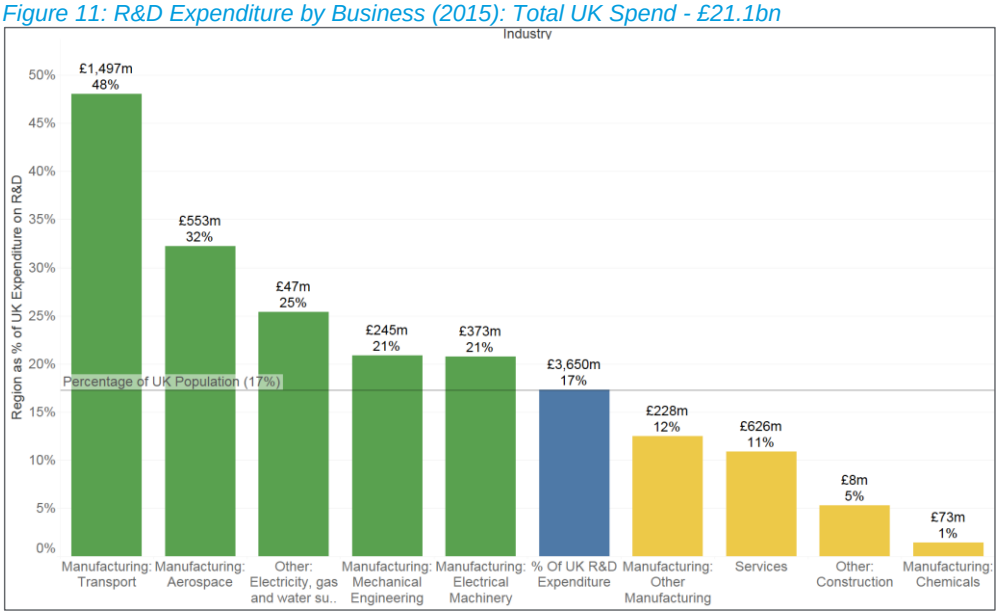
[26] R&D expenditure data is best available at the level of NUTS2 regions

[27] ONS, *Gross domestic expenditure on research and development, by region, UK.* 2018. Available at: https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/datasets/ukgrossdomesticexpenditureonresearchanddevelopmentregionaltables

In 2015, an estimated £4.67bn of R&D expenditure was undertaken in the West Midlands and South West (15% of UK R&D expenditure), of which £3.65bn (78%) was made by business, £800m (17%) by higher education and £220m (5%) by government. Within the region, businesses contribute a greater proportion of total R&D expenditure (78%) than the UK rate (66%), with a correspondingly lower proportion coming from higher education (17% v 25%) and government (5% and 7% respectively).

Further analysis (Figure 11) of Business Expenditure on Research and Development (BERD) for the West Midlands and South West indicates the relative strength in expenditure made within the manufacturing sectors. The two regions contribute almost half (48%) of the UK's overall BERD in transport, a third of BERD in aerospace manufacturing, and is also strong in electricity, gas and water supply, engineering and machinery.

Figure 11: R&D Expenditure by Business (2015): Total UK Spend - £21.1bn



Source: Data compiled by Technopolis based on ONS UK government expenditure on science, engineering and technology (June 2017).

4. CYBER RESILIENCE

4.1 Introduction:

4.1.1 Defining Cyber Resilience

For this Audit, we draw upon the Singer and Friedman (2014) definition of cyber resilience. This is further well captured by the NCSS which recognises that resilience within UK organisations goes in hand with trust which underpins a successful digital economy.

"Resilience is what allows a system to endure security threats instead of critically failing. A key to resilience is accepting the inevitability of threats and even limited failures in your defences. It is about remaining operational with the understanding that attacks and incidents happen on a continuous basis. Short of pulling the plug, there is no such thing as absolute security."

Singer, P W and Friedman, A (2014) Cyber Security and Cyber War

"Our economy, the administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. **A loss of trust in that integrity would jeopardise the benefits of this technological revolution... systems and technologies that underpin our daily lives – such as power grids, air traffic control systems, satellites, medical technologies, industrial plants and traffic lights – are connected to the Internet and, therefore, potentially vulnerable to interference.**"

National Cyber Security Strategy 2016-2021

4.1.2 UK Government: National Cyber Security Strategy 2016-21

The National Cyber Security Strategy (2016-21) is a pivotal strategy for the Cyber Resilience Alliance. It sets out proposed investment of £1.9bn in supporting the cyber security sector, and its innovation, research and development over the five years. It recognises that whilst the initial National Cyber Security Strategy (2011) was beneficial in helping the UK become a leading global player in cyber security, there is more to achieve in the years ahead, including:

- Too many networks, including in critical sectors, are still insecure.
- The market is not valuing, and therefore not managing, cyber risk correctly.
- Too many organisations are still suffering breaches at even the most basic level.
- Too few investors are willing to risk supporting entrepreneurs in the sector.
- Too few graduates and others with the right skills are emerging from the education and training system."[28]

[28] HM Government, *National Cyber Security Strategy 2016-2021*, pg 27. 2016. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

To address these issues, the NCSS sets out three core themes:

Theme	National Ambition	Cyber Resilience Alliance
Defend: 	"We have the **means to defend the UK against evolving cyber threats**, to respond effectively to incidents, to ensure UK networks, data and systems are **protected and resilient**. Citizens, businesses and the public sector have the knowledge and ability to defend themselves."	The Cyber Resilience Alliance are home to: • Over [80] businesses dedicated to cyber security product and service provision; • Knowledge Sharing is crucial to UK network defence: we have many clusters dedicated to risk and knowledge sharing (Malvern, Cynam, CGP members); • Local Enterprise Partnerships committed to the dissemination of good business practice in cyber security and resilience (e.g. ISO / Cyber Essentials accreditation, sharing of NCSC guidance).
Deter: 	"The UK will be a **hard target for all forms of aggression in cyberspace**. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so."	We are home to GCHQ in Cheltenham, and the Ministry of Defence Cyber Unit in Corsham. We also host a wide range of national security firms including BAE Systems Applied Intelligence, QinetiQ, and Lockheed Martin.
Develop: 	"We have an **innovative, growing cyber security industry, underpinned by world-leading scientific research and development**. We have a **self-sustaining pipeline of talent** providing the skills to meet our national needs across the public and private sectors. Our **cutting-edge analysis**	The Cyber Resilience Alliance is committed to the development of the industry in a wide range of ways including: • **Getting the infrastructure right:** We have demonstrated a clear commitment to the development of dedicated infrastructure for the growth of cyber businesses e.g. Cheltenham Cyber Park (£22m), the Berkeley C11 Cyber Security Centre (£3m), Hereford's Enterprise Zone etc. We also are host to the Ark Data Centres, which provide the secure hosting necessary to grow the UK's digital economy. We remain committed

	and expertise will enable the UK to meet and overcome future threats and challenges."	to providing the affordable and secure space needed for the sector, and will be key to supporting the sector's requirements[29] • **Supporting our Universities and Further Education:** We will support the ongoing development of BSc and MSc courses in Cyber Security, and support Degree Apprenticeships in the region. Given the businesses in the region, we will seek to continue working collaboratively to identify business and public need from course delivery. • **Developing and Enabling Clusters:** Many of the UK's leading cyber security clusters (UK Cyber Security Forum, with c. 600 national members) and CyNam are active in the region and share sectoral knowledge and promote collaborative relationships. • **Engaging with national policy-leads:** We are known by the NCSS and its lead departments (Cabinet Office, DCMS, DIT) as a leading cluster. • **Promoting inclusivity in the sector:** We recognise that cyber security consists predominantly of men (89%)[30], and that there are challenges in breaking down barriers to accessing employment in the sector for many social groups. We will back initiatives that enable access and diversity.

We are a leading region in cyber security, and we will endeavour to support the ambitions of the National Cyber Security Strategy. Further, in order to 'defend, deter and develop', it is also necessary to validate new cyber security products, processes and solutions in a secure lab prior to utilising these within the event of a cyber-attack or prevention. This demonstrates the real benefit in validation facilities that meet market and public defence requirements to accelerate high-quality product development, and to conduct world-leading research and development to defend the UK, deter threats, and develop innovative applied solutions.

[29] Savills, *Cybersecurity firms set to take 1m sq ft of UK office space as rise in tech leads to greater threat.* Available at: http://www.savills.co.uk/_news/article/72418/228713-0/3/2018/cybersecurity-firms-set-to-take-1m-sq-ft-of-uk-office-space-as-rise-in-tech-leads-to-greater-threat

[30] Peacock, D, & Irons, A, 2017. Gender Inequalities in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression. International Journal of Gender, Science and Technology, [Online]. Vol. 9, No. 1, 11111. Available at: http://genderandset.open.ac.uk/index.php/genderandset/article/viewFile/449/824

4.1.3 Embedding Cyber Resilience & Supporting National Security

This section sets out our role in embedding cyber resilience in the region and wider UK, and our capability and contribution in helping to secure the UK's digital economy.

The implications and cost of cyber-attack (i.e. compromised networks, loss or theft of data), is often experienced and amplified through the lack of suitable planning, back-ups and contingency in place among businesses and UK organisations. For example, in a ransomware attack, many organisations are faced with a choice: to pay a ransom and have their data unencrypted, or to face deletion of the contents of their hard drive or network. Where firms have suitable back-ups and a clear approach in place, the 'cost' of ransomware may be lower than for those that may feel they have no effective 'Plan B'.

The DCMS Cyber Security Breaches Survey (2018) sets out the challenges that UK organisations face in securing their organisations and mitigating their cyber security risks. For example:

- 98% of all UK businesses and 93% of charities are reliant on online services;
- **Over four in ten (43%) of all UK businesses have experienced cyber-attacks or breaches in the last 12 months, and this figure rises to 72% among large[31] businesses.**
- Not all experiences of cyber breaches result in a business impact (e.g. the need to implement new measures, staff time needed to deal with the breach, or prevention of day-to-day work). However, more than half (53%) of attacks do result in a specific material or financial cost for businesses.
- In 2017**, the average cost of such breaches is £3,100.**

With regard to basic practice, there are clear gaps in cyber resilience practices in UK organisations. The UK Cyber Security Breaches Survey (2018) demonstrates that **only 51% of UK businesses and 29% of charities have implemented the five basic technical controls** under the Government endorsed Cyber Essentials scheme:

- Applying software updates when available (92% of businesses and 75% of charities)
- Up-to-date malware protection (90% and 73%)
- Firewalls with appropriate configurations (89% and 69%)
- Restricting IT admin and access rights to specific users (78% and 65%)
- Security controls on company-owned devices (65% and 42%).

Furthermore, 34% of micro and small businesses in the UK reported to be spending £0 on their cyber security.

[31] Over 250 employees.

Table 3: Cyber Security Breaches Survey 2017 Average Investment in Cyber Security in Last Financial Year

	All businesses	Micro/small	Medium	Large
Median Spend	£200	£200	£5,000	£21,200
Base	1,209	829	268	112
% of firms spending £0		34%	13%	9%

Source: DCMS Cyber Security Breaches Survey (2017)[32]

This means there are approximately 750,000 firms (employing at least one employee) across the UK that are not investing in cyber security exposing the UK to significant operational, economic and social risks. We recognise the scale of this shared challenge in the need to make cyber security affordable, accessible, and a basic part of organisational hygiene. The Cyber Resilience Alliance is home to innovative products, services and standards (e.g. IASME), and we will draw upon the significance of our cyber security community to embed cyber resilience for the whole community, from the individual level to the largest businesses, health trusts, and organisations.

However, cyber resilience is for all organisations to embrace and to adapt. Larger organisations are often subject to an intense number of attacks given the potential 'prize' of attack (demand for ransoms, reputational damage from data loss etc.) with large companies in the UK having an average of 6,490 (and median of 12)[33] attempted breaches in 2017 alone (DCMS) indicating that some large businesses are particularly targeted.

Within the Cyber Resilience Alliance, we are home to a number of defence, security, and manufacturing firms crucial to the smooth running of the nation, in addition to our health and emergency services. It is therefore of national importance that resilience to attacks is a core investment in all business and public service planning.

In line with the principles of the National Cyber Security Strategy, we identify a wide range of public assets that we will draw upon in supporting national cyber security.

[32] Department for Digital, Culture, Media and Sport, Ipsos MORI Social Research Institute and University of Portsmouth, *Cyber Security Breaches Survey 2017: Statistical Release*. 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

[33] Department for Digital, Culture, Media and Sport, Ipsos MORI Social Research Institute and University of Portsmouth, *Cyber Security Breaches Survey 2018: Statistical Release*. 2018. Sourced from Table 5.1. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Securing our Digital Economy:	Value Proposition
Embedding Cyber Resilience in UK businesses and organisations	The Cyber Resilience Alliance is home to a wide range of organisations that complement the provision of cyber resilience (provision of anti-virus and anti-malware solutions, penetration testing, risk and threat detection and monitoring) in business and public services. The region is also home to the IASME Consortium in Malvern, which is one of only five companies appointed as Accreditation Bodies for assessing and certifying the Government's Cyber Essentials Scheme. **This means that the implementation of the five basic technical controls is being promoted directly from the Cyber Resilience Alliance.**
Securing Critical National Infrastructure[34]	The Government defines CNI as the assets, facilities, systems, networks or processes which, if lost or disrupted, would affect national security or the delivery of essential services, leading to severe economic or social consequences or loss of life.[35] The majority of UK CNI is privately owned.[36] The Government says that the responsibility for managing cyber risk in private sector CNI lies with the operators, but that it will monitor and ensure CNI cyber security, working with private operators through a variety of channels. With several firms providing CNI security solutions (BAE Systems Applied Intelligence, QinetiQ etc), and public organisations including GCHQ / NCSC, the Ministry of Defence investments in cyber capability (e.g. Global Operations and Security Control Centre in Corsham[37]) – **we are core to addressing vulnerabilities in Critical National Infrastructure across the UK and providing the firms and organisations with the solutions to meet the challenges of legacy systems.**

[34] Parliamentary Office of Science & Technology, *Cyber Security of UK Infrastructure*. May 2017. Available at: http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf
[35] Cabinet Office, *Summary of the 2015-16 Sector Resilience* Plans. April 2016. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/526351/2015_16_summary_of_the_srp.pdf
[36] Intelligence and Security Committee, *Foreign involvement in the Critical National Infrastructure-The implications for national security*. June 2013. Available at: https://www.parliament.uk/documents/other-committees/intelligence-security/Critical-National-Infrastructure-Report.pdf
[37] GOV.UK, *UK steps up cyber defence*. 2018. Available at: https://www.gov.uk/government/news/uk-steps-up-cyber-defence

Enabling Infrastructure	The Cyber Resilience Alliance is committed to the provision of dedicated infrastructure and support to enable the growth of cyber security in the region: **Growing and Supporting Research and Ideas:** The Cyber Resilience Alliance is home to two universities providing cyber security courses (University of Gloucestershire, and University of Worcester). UK Research & Innovation (UKRI), with a combined research budget of £6bn per annum is also based in Swindon, providing proximity and ease of access of our universities and businesses to the home of UK research and innovation. **Access to Capital:** The Cyber Resilience Alliance covers four LEP areas, and there is recognition that there is a regional imbalance in funding (London and South East) and access to capital for SMEs. There are several grant and loan funding initiatives within the region for supporting cyber security businesses, in addition to private routes to capital for firms e.g. venture capital investment and private lending. Most recently, the Midlands Engine Investment Fund (February 2018) announced a further £100m in equity finance provision – increasing on the £1.2bn of finance provided by the British Business Bank to Midlands firms. However, there is recognition by the Cyber Resilience Alliance that more can be done to provide access to funding for cyber start-ups and growth prospects. **Investing in Physical Infrastructure:** The Cyber Resilience Alliance is undergoing direct investment in physical infrastructure to enable the growth of the sector. Savills estimate that as much as 1 million sq. ft of office space will be taken by cyber security firms over the next five years (by 2023)[38] The upcoming investments in the Cheltenham Cyber Park (£22m, up to 7,000 jobs) and the Marches Centre for Cyber Security (£9m, 185 jobs), the Malvern Hills Science Park (Phase Five development, £4m) and the outcomes from existing investments in incubation (e.g. GCHQ Cyber Accelerator, and the LEP Growth Hubs) offer real space and potential for growth.

[38] Savills, *Cybersecurity firms set to take 1m sq ft of UK office space as rise in tech leads to greater threat.* Available at: http://www.savills.co.uk/_news/article/72418/228713-0/3/2018/cybersecurity-firms-set-to-take-1m-sq-ft-of-uk-office-space-as-rise-in-tech-leads-to-greater-threat

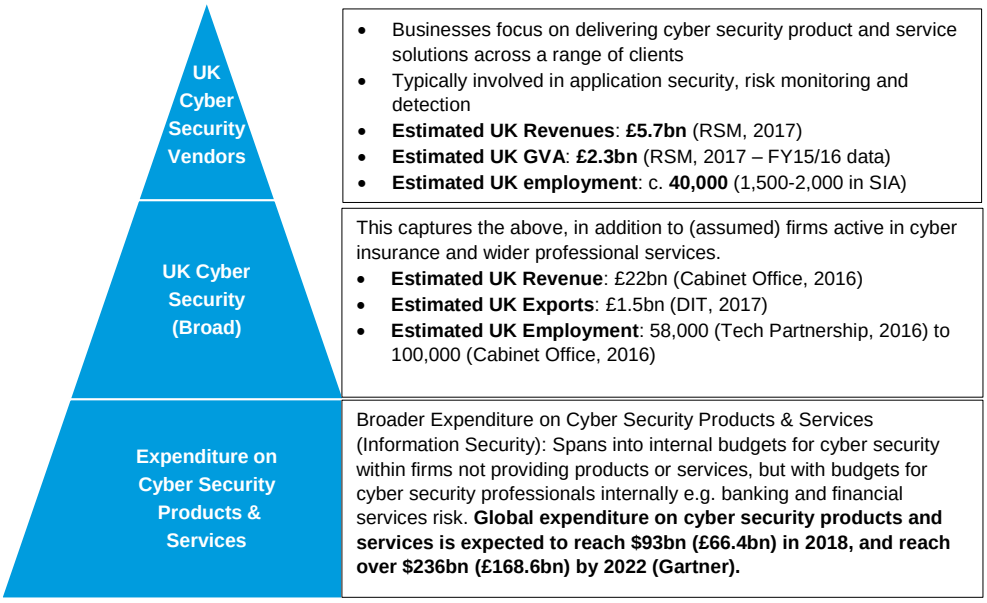
	Conceptual Layout for the Cheltenham Cyber Park  Further, the region offers the physical infrastructure required for enabling digital growth, including the Ark Data Centre at Corsham, and Shield House in Gloucester. The region also is committed to further enhancement of SuperFast broadband (e.g. Fastershire initiative), and in March 2018, Worcestershire LEP was also awarded funding to deliver one of six 5G Testbed trials, signalling its commitment to transformation of UK mobile technology and productivity.
Talent Pipeline	The region is also committed to supporting innovative schemes for encouraging new talent into the sector through its involvement in supporting Degree Apprenticeships, skills opportunities – e.g. Cyber Security Challenge; conversion courses e.g. SANS Institute; inclusive delivery of skills e.g. Security Operations Centre in Worcester for neurodiversity; and involvement with national initiatives (Cyber Schools Programme, Institute of Coding, and Cyber Security Skills Immediate Impact Fund).

4.2 National and International Trends and Size of Global Markets

4.2.1 Introduction

The cyber security market is synonymous with high growth, expansion and investment in the United Kingdom. However, the definition of the 'cyber security market' shapes the assumptions regarding potential revenues, Gross Value Added (GVA), and employment within the market. To analyse the market in a meaningful way regarding targeting and market development, it is best to think of three layers, as set out below for the UK market:

Commented [DS1]: https://www.gov.uk/government/news/cyber-skills-for-a-vibrant-and-secure-uk - If no DCMS, use this - £6bn



Source: RSM, Cabinet Office[39], Gartner[40]

Key Market Analysis Knowledge:

- The Cyber Security 'market' does not have a formal agreed definition and is continually shifting – particularly as cyber security spending and functions become more embedded in more 'traditional' industries e.g. automotive, financial services, retail, transport, energy and health. However, as set out by Gartner's global market research, the procurement of cyber security products and services is clearly an area in which there is **robust revenue and employment growth (estimated >10% CAGR),** driven by proliferation of cyber risk and direct government policy (potential for fines for companies failing to meet obligations regarding information security).

[39] 100,000 employed: Cabinet Office (UK Cyber Security Strategy 2011-16, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf)

[40] https://www.gartner.com/en/information-technology/insights/cybersecurity

- There are clear opportunities for sectoral support in embedding cyber resilience that will result in commercial outcomes for the region. This means developing secure solutions that can be used widely (e.g. threat monitoring, anti-spam/malware/virus solutions), as well as firm and sector specific interventions e.g. securing autonomous vehicles (as evidenced in the Connected Midlands project), securing CNI and supporting national defence and offensive capabilities. Further, the maturity of the Cyber Resilience Alliance and wider UK market is known to be world-leading (with the UK, USA and Israel as the 'top three' markets[41]). This provides considerable export opportunities.

4.2.2 Market Trends: National and International

The cyber security market is difficult to measure given significant subjectivity in definition and inclusion of value; for example, should (and if so, how) the value of an application of Microsoft Defender be measured within context of the wider operating system (Windows 10), or how might the investment placed in securing autonomous vehicles be best captured? Estimates of the cyber security market to date have tended to focus on two approaches, namely:

Identifying Business Growth:

- This can be examined through measuring the revenues, Gross Value Added and employment of firms which attribute much of their revenues to cyber security product and service provision. For example, this includes firms which are recognised as being a 'cyber security firm' often reflected through accreditation and memberships of cyber security clusters e.g. Titania, Anon.AI. Where firms are large and diversified in nature (e.g. BT, Cisco, HP, Airbus etc.), this requires further analysis setting out the proportion of a firm's earnings linked to cyber security product and service sales. RSM analysis (2017) of over 800 cyber security firms in the UK identified UK revenues of c. £5.7bn. RSM analysis demonstrates that in the past five years (2012-17), the number of firms active in the sector in the UK has grown by almost 50%, with over 100 new business registrations in the market within the past two years, representing a surge in new entrants to the market.
- In 2013, Pierre Audoin Consultants[42] conducted a similar exercise on behalf of BEIS, which identified approximately 600 firms with £2.8bn in revenue. In 2013, this exercise identified QinetiQ and BAE Systems (both active within the Cyber Resilience Alliance) as key to export growth in cyber security. Further, it identified the potential of the region's SME base highlighting that Titania, generated more than 80% of its revenues from exports.
- DIT also view cyber security as a key export opportunity for the UK. The most recent statistics set out that cyber security accounted for £1.5bn of UK exports in 2016[43], which reflects approximately a third of UK security exports, and is expected to grow approximately 12% per annum over the next five years (2021).

Commented [DS2]: as previous

[41] PwC (2015) https://www.pwc.com/sg/en/publications/assets/unlocking-cybersecurity-growth-potential.pdf
[42] Pierre Audoin Consultants, *Competitive analysis of the UK cyber security sector.* 2013. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf
[43] Department for International Trade & Defence & Security Organisation, *UK Defence & Security Export Statistics for 2016*. 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/631343/UK_defence_and_security_export_statistics_2016_Final_Version.pdf

Examining Cyber Security Expenditure:
It is recognised that the value of the sector in the UK is also driven by other factors including internal expenditure of firms e.g. internal projects, and recruitment of security staff (e.g. Chief Information Security Officers), and public expenditure e.g. government spending on cyber security solutions, and university expenditure.

Gartner: With regard to absolute values in IT and cyber security budget and expenditure within firms, Gartner (2016)[1] has identified that global IT spending (including internal and external functions) reached $3.41tn in 2016, of which 5.3% is within the UK. Based on an average 2016 exchange rate of £1.36: £1 (XE), **IT budgets across all sectors in the UK are estimated at £132.9bn per annum**.

Gartner also provide a breakdown on IT security spending as a percentage of IT budgets. They note the difficulty in estimating this figure as many firms find it challenging to proportion their IT budget into subcategories e.g. security may be an 'in-built' component of a contract, rather than a direct purchase. As a result, they estimate that IT security spending as a percentage of business IT budgets ranges from 1 – 13%, but on **average is 5.6% (for every £1,000 of IT budget, a firm can be expected to spend approximately £56).** This provides an estimated average cyber security budget for UK firms of £1,306 annually, and **total cyber security budgets of £7.4bn per annum.**

Projected Market Growth:
Market projections reflect an estimate of how the market might reasonably be expected to perform in upcoming years and can shape and be shaped by market confidence and investment. There are a wide range of estimates from market intelligence firms, summarised below:

Intelligence	Market	Projected Growth (CAGR[44])
Gartner	Worldwide Information Security Spending	**8%** (2017 to 2018)[45]
BusinessWire	Global Cybersecurity Market	**11%** (2017 to 2022)[46]
Cyber Security Ventures	2018 Cybersecurity Market Report	**12-15%** (2017-21)[47]

[44] Compound Annual Growth Rate
[45] Gartner, *Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017*. Available at: https://www.gartner.com/newsroom/id/3784965
[46] Neuways, *Cyber Security Market to grow from $137.85 Billion in 2017 to $231.94 Billion by 2022.* Available at: https://www.neuways.com/neutech/cyber-security-market-to-reach-231-9-billion-by-2022/
[47] Cybersecurity Ventures, *2018 Cybersecurity Market* Report. Available at: https://cybersecurityventures.com/cybersecurity-market-report/

There are also a small number of cyber security submarkets of relevance to the region, including:

Intelligence	Sub-market	Projected Growth
Radiant Insights	Global **Automotive** Cyber Security Market	**28%** (2017 to 2021)[48]
Report Linker	**Smart Grid** Cyber Security Market	**13%** (2018 to 2022)[49]
Technavio	Global **IoT** Security Market	**55%** (2016 to 2020)[50]

The UK Cyber Security Strategy sets out that the Government will measure its success in stimulating growth in the cyber security sector by assessing progress towards the following outcomes:

- greater than average global growth in the size of the UK cyber sector year-on-year;
- a significant increase in investment in early stage companies;
- adoption of more innovative and effective cyber security technologies in government.

In line with the National Cyber Security Strategy's ambition to exceed average global growth (CAGR) in the cyber sector, it is estimated that as a strong cluster of cyber activity in the UK, the **Cyber Resilience anticipates and will plan interventions within the sector assuming annual growth of 10% per annum (in revenue and employment).**

[48] Radiant Insight, *Global Automotive Cybersecurity Market 2017-2021*. 2017. Available at: https://www.radiantinsights.com/research/global-automotive-cybersecurity-market-2017-2021?utm_source=Referral&utm_medium=abnewswire&utm_campaign=Jyoti
[49] Cision, *Smart grid cybersecurity market is projected to grow at a CAGR of 13% by 2022*. Available at: https://www.prnewswire.com/news-releases/smart-grid-cybersecurity-market-is-projected-to-grow-at-a-cagr-of-13-by-2022-300621845.html
[50] Research Moz, *Global Internet of Things Security Market 2016-2020*. 2016. Available at: https://www.researchmoz.us/global-internet-of-things-security-market-2016-2020-report.html

4.2.3 Size and Scale of the Cyber Resilience Alliance's Cyber Sector

The UK cyber security sector is a world-leader, alongside the United States and Israel, and has the largest cyber security market in Europe, with an estimated 5.3% global share.[51]

Within the UK itself, London is recognised as a cyber security hotspot, with more than two hundred cyber security firms estimated in the city[52], with many more vying for cyber security talent to support the operations and development of financial services, legal services, media and telecommunications etc.

However, the Cyber Resilience Alliance Science and Innovation Audit has **enabled an overview of the firms and organisations active within the region and provides an evidence base that the region reflects the second largest cluster of cyber security activity outside of London. This, combined with the extent of research & development, and wider innovation, demonstrates the role of the region as a key UK cluster for cyber security.**

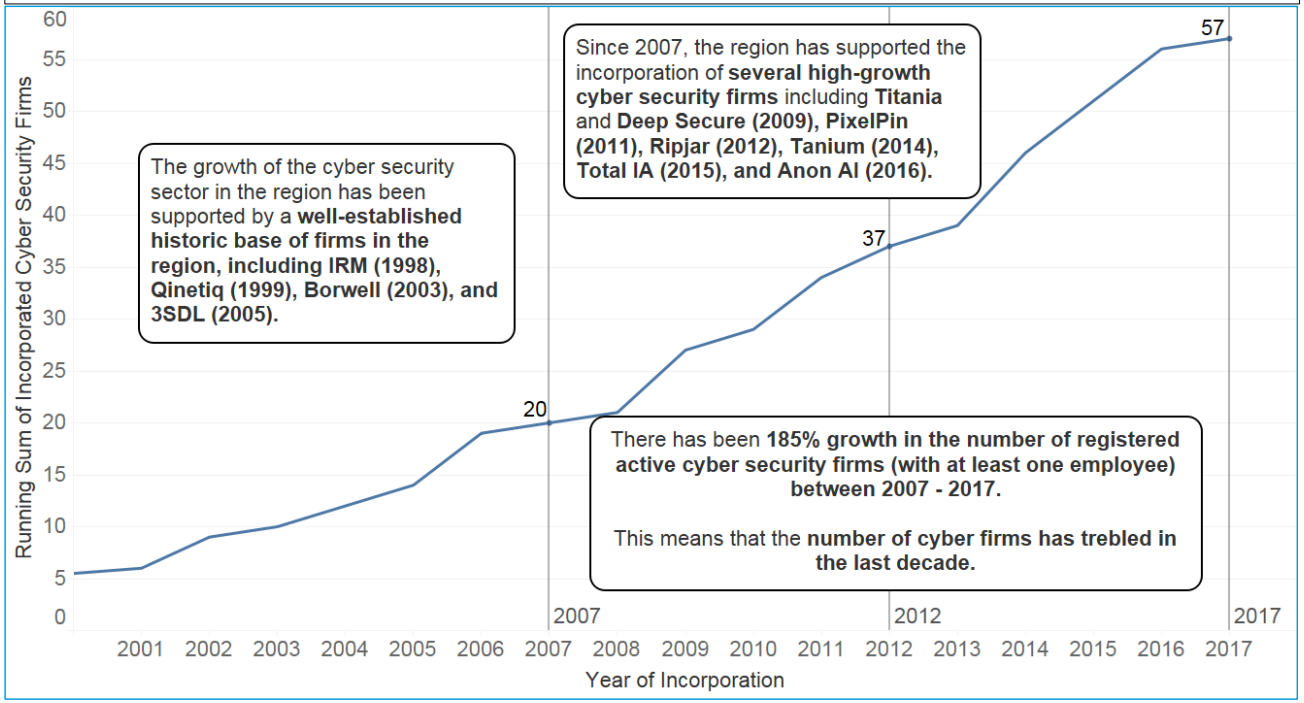
An overview of firms known to be active in the sector within the four Local Enterprise Partnerships, in addition to business registration data[53], indicates that:

- The region contains over a hundred organisations (public and private) involved in cyber security.
- Approximately **eighty firms are** actively engaging in the cyber security sector;
- Of these, we estimate that **fifty-seven (see Fig 13 overleaf)** are dedicated providers of cyber security products and services, and a further twenty-one are 'diversified'.[1]
- DIT estimate there are approximately 800 cyber security firms operating in the UK[1], which means an estimated **8-10% of these are active in the Cyber Resilience Alliance.**
- Furthermore, the CyberExchange Directory identifies approximately eighty active firms in the wider West Midlands & South West.
- This audit also recognises that the significant membership of local cyber security clusters, including Malvern Cyber Security Cluster (c. 80 members), West of England Cyber Cluster (c. 200 members), and the role of individual contractors and non-incorporated start-ups means these figures could be considered conservative.

[51] Gartner, *Gartner Says IT Spending in EMEA to Exceed $1 Trillion in 2018, Up 4.9 Percent from 2017*. Available at: https://www.gartner.com/newsroom/id/3825563
[52] CyberExchange Map, Accessed May 2017.
[53] Bureau van Dijk Orbis.

Fig 13: Running Count of Firms Incorporated Dedicated to Cyber Security Product / Service Provision within the Cyber Resilience Alliance:

Source: Bureau van Dijk



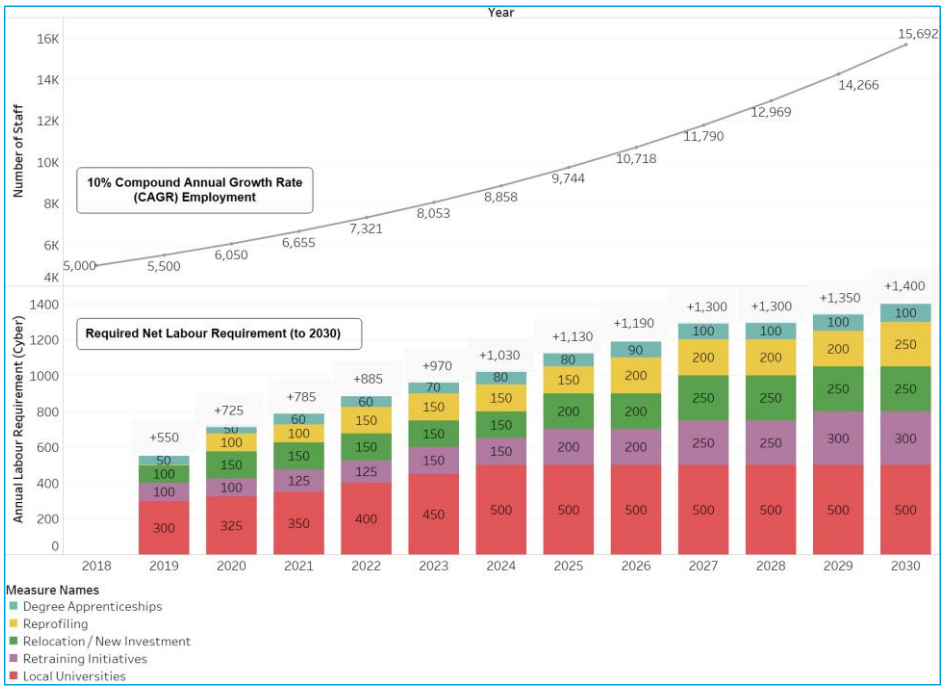
4.3 Employment Estimates and Projections:

RSM estimate there are approximately 2,000 employed in the region's direct (private) cyber security sector and aligned industries (defence and security etc.). However, the region is also home to an estimated 6,000 employees in GCHQ, and 2,000 in the MoD (Corsham). **Therefore, consultees throughout this exercise have suggested that the cyber security sectoral employment in the region may be in the region of c. 5,000 FTE employees, with cyber security crossing several core employment sectors.**

This consists of an estimated 5,000 employed in the cyber security sector in the region (of which approx. 3,000 in public sector). UK estimates of employment in cyber security range from 40,000 (private estimate – RSM for DCMS), 58,000 (Tech Partnership), to 100,000 (Cabinet Office).

The Cyber Resilience Alliance represents 5% of UK sectoral employment (conservative estimate). Given the working-age population of the region is 3.9% of the UK total, this provides a LQ of 1.29, evidencing the region's strength in cyber.

Fig 14: Anticipated Sectoral Growth (in employment) and net labour requirement estimate



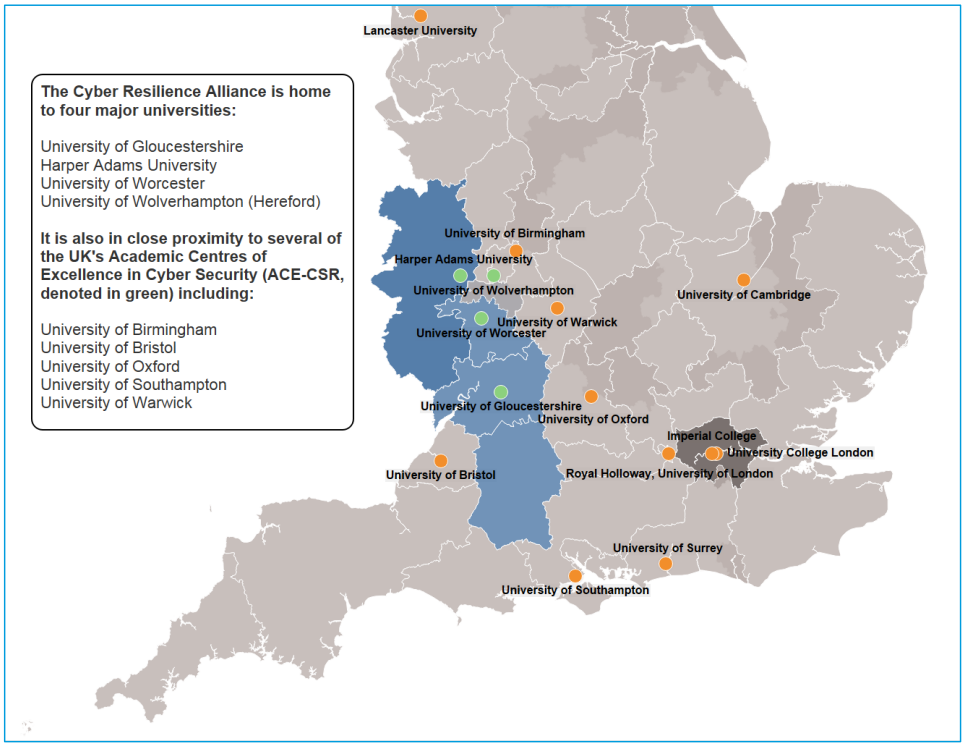
Source: RSM / Cyber Resilience Alliance

4.4 Local Science and Innovation Assets

The region is focused upon developing its entrepreneurial and innovation support network, with emphasis on high-tech, cyber, digital and manufacturing industries. The region is home to a wide range of universities, research institutes and councils, public sector organisations, businesses, and incubation and innovation space active within developing the cyber security sector. This Audit has identified over a hundred assets and organisation active in supporting cyber security product and service development. Further, the region is in close proximity to several world-leading businesses, universities and research institutions active in cyber security, advanced manufacturing and automotive technologies. This section sets out a profile of the region's university base, public (research intensive) organisations, and sectoral initiatives to develop the sector in the region.

4.4.1 Universities:

Fig 15: Universities within the Region: (Note green = internal to region, orange = Academic Centre of Excellence in Cyber Security Research)



Source: RSM, EPSRC

Analysis of the region's university base has indicated that the region offers strengths with regard to:

- Significant and growing provision of cyber security (and related)[54] courses at undergraduate and postgraduate level, helping to tackle the skills gap;
- Engagement with business community in course and facility design e.g. University of Gloucestershire and the C11 Cyber Security and Digital Centre at Berkeley Green;
- Close proximity to several of the UK's leading accredited Academic Centres of Excellence in Cyber Security Research (ACE-CSRs), enabling business and academic partnerships in the region;
- Accreditation of courses alongside higher and further education providers (e.g. Working in conjunction with the Heart of Worcestershire College, the University of Worcester also offers a foundation degree in cyber security)

University	Research Excellence Framework 2014[55]	Teaching Excellence Framework (2017)[56]	Cyber Security Presence[57]
University of Gloucestershire	= 98th	Silver	Yes (BSc Hons in Cyber and Computer Security / MSc Cyber Security)
University of Worcester	= 117th	Silver	Yes (modules within BSc Computing), Foundation Degree in Cyber Security
University of Wolverhampton	= 105th	Bronze	Yes (BSc Hons Cyber Security / MSc Cyber Security and Digital Forensics). Involved in Marches Centre for Cyber Security.
Harper Adams University	= 19th[58]	Gold	Limited: Provision of MSc Automotive Engineering / MSc Agricultural Engineering
Adjacent to SIA Region:			
University of Birmingham	=31st	Gold	ACE-CSR Status, Certified (NCSC) MSc in Cyber Security
Coventry University	75th	Gold	Offers an MSc in Cyber Security / Provides Ethical Hacking facilities
University of Warwick	8th	Silver	ACE-CSR Status, provisionally Certified Master's Degrees in Cyber Security Engineering/ Cyber Security and Management.
Cranfield University	=31st	Did Not Participate	Offers a provisionally Certified Master's Degree in Cyber Defence and Information Assurance.
University of Bristol	=11th	Silver	ACE-CSR Status
University of South Wales	=93rd	Did Not Participate	Offers a provisionally Certified Master's Degree in Computer Forensics

[54] Includes Computer Science, Information Technology, Computing, and Mathematics and Physics
[55] Sourced via: https://www.timeshighereducation.com/sites/default/files/Attachments/2014/12/17/k/a/s/over-14-01.pdf
[56] Times Higher Education World University Rankings, *Teaching excellence framework (TEF) results 2017*. 2017. Available at: https://www.timeshighereducation.com/news/teaching-excellence-framework-tef-results-2017
[57] Provides teaching or research.
[58] 19th out of 26 Single Subject Institutions

Case Study: Universities in the region (within the Cyber Resilience Alliance)

The University of Gloucestershire, University of Worcester, and University of Wolverhampton offer cyber security specific courses at both an undergraduate and postgraduate level. Recently, the University of Gloucestershire was announced as being a partner to the Institute of Coding which was highlighted by Theresa May within the 2018 World Economic Forum in Davos as being a key part of the Government's initiatives in reducing the digital skills gap[14].

One of the most popular courses offered by the University of Gloucestershire is the BSc Cyber and Computer Security degree. The University of Gloucestershire also offers BSc Computer and Cyber Forensics[16] as well as a MSc Cyber Security[17] course; ultimately producing high quality graduates which local companies can utilise. These courses are supported by the University's Institute of Cyber and Risk Assessment whose applied research and knowledge exchange activities inform the teaching programmes and provide a basis of a service to business.

The University of Wolverhampton hosts a BSc Cyber Security course, from which 87% of graduates find full time employment or education within six months of graduation. The University recently (February 2018) secured £192,000 of funding to develop its cyber security course offer, including the development of a new MSc in Cyber Crime which will be designed to appeal to anyone with working experience in the area from entrance level up to established consultants and practitioners. It will be designed using CyberKombat - a cybersecurity modelling, development training, testing and certification environment which mimics real world security architectures and operations centres. The Wolverhampton Cyber Research Institute was also set up by the University in 2017 and aims to become a world leading multi-disciplinary Cyber Research Centre of Excellence, focusing on Secure Healthcare, Transport including Automotive, Aviation and Secure Space; Secure infrastructure for sustainable cities; and Security for smart power grids.

The University of Worcester adds to this pool of graduates through its BSc (Hons) Computing course, covering a variety of skills applicable to Cyber Security operations directly. Furthermore, universities in the region are expected to continue to invest in cyber security course and facility development in the coming years (see Section 5.4). The region is also expected to become host to the first brand new UK university in over thirty years – 'the New Model in Technology and Engineering (NMITE) which will focus on practical learning involving industry and public partners. It is expected to take 300 students in its first year (2018) but grow to 5,000 over the following decade and is expected to provide courses in cyber security.[59]

University of Worcester
UNIVERSITY OF WOLVERHAMPTON
KNOWLEDGE • INNOVATION • ENTERPRISE
UNIVERSITY OF GLOUCESTERSHIRE

[59] New Model in Technology & Engineering, available at: http://nmite.org.uk/

4.4.2 Government:

In addition to the University base, the region is also home to a several nationally and internationally significant public bodies with respect to defence, security and research. These include:

Defence and Security:

GCHQ: The Government Communications Headquarters (GCHQ) is a UK intelligence and security organisation that provides signals intelligence and information assurance to the government and security services. It is headquartered in Cheltenham with their site there being home to around 4,000 employees. Sitting within GCHQ is the National Cyber Security Centre (NCSC), an organisation that provides advice to support to the public and private sector in how to avoid computer security threats. Some of the NCSC's operations take place at the Cheltenham headquarters, forming a central part of the SIA area's cyber security cluster.

Working with HMG and industry, GCHQ defends Government systems from cyber threat, provide support to the Armed Forces and strive to keep the public safe, in real life and online. GCHQ continues to play a key role in Strategic Defence and Security Review (SDSR), where the Government has committed to invest £1.9 billion over five years in protecting the UK from cyber-attacks and developing our sovereign capabilities in cyber space. GCHQ work closely with allied agencies such as the US National Security Agency (NSA) and the US Department of Defense (DOD).

Ministry of Defence (MOD) Joint Cyber Unit (Corsham / Cheltenham), Global Operations and Security Control Centre (Corsham), Defence Fulfilment Centre (Telford)

One such Cyber Corridor organisation is MOD Corsham in Wiltshire, where in 2016 as part of the SDSR and in a move to further strengthen the UK's cyber defences, the former Defence Secretary Michael Fallon announced that over £40 million will be spent on a new Cyber Security Operations Centre (CSOC) to protect the MOD's cyberspace from malicious actors. The CSOC will work closely with the National Cyber Security Centre to facilitate the sharing of MOD cyber security challenges and contribute to wider national cyber security.

Defence Science and Technology Laboratory (DSTL): The DSTL headquartered in Porton Down, Wiltshire is an executive agency of the MOD and one of the principal government organisations dedicated to science and technology in the defence and security field. DSTL supply specialist services to the MOD and wider government. 60% of MOD's science and technology programme (total funding: £410 million) is supplied by external partners in industry and academia worldwide. (APMG International is working with Dstl and Ploughshare Innovations Ltd, Dstl's technology transfer company, to deliver a new Cyber Defence Capability Assessment Tool (CDCAT®)[60] Dstl has also been working with the Alan Turing Institute to develop machine learning technology for cyber security.[61]

[60] Defence Contracts Online, *Protecting the UK from cyber-attack*. Available at: https://www.contracts.mod.uk/features/protecting-the-uk-from-cyber-attack/
[61] UK Authority.com, *UKA Cyber Resilience*. Available at:http://www.ukauthority.com/cyber-resilience/entry/7950/dstl-explores-machine-learning-for-cyber-security

Cyber Corridor Defence and Security Eco-System

Thanks to these critical organisations being based within the Cyber Corridor, there is a strong supporting eco-system of innovative Cyber and Security companies both large such as Bae, QinetiQ, Northrop Grumman and Raytheon and SMEs such as Titania Limited, 3SDL & Borwell. This in turn ensures that there is a large and well qualified and experienced Defence and Security workforce to support and continue to drive the region's innovation.

The **Special Air Service (SAS) Regiment and the associated Signals Regiment** are also based in Hereford.

Research & Innovation

The region is home to UK Research and Innovation (UKRI): formed in April 2018, this has a combined budget of more than £6bn and includes the former research councils (AHRC, BBSRC, EPSRC, ESRC, MRC, NERC, and STFC), Innovate UK, and Research England. It is also host to the UK Space Agency in Swindon, at the heart of UK efforts to explore and benefit from space expedition and research. Government has also committed to further investment in the cyber security sector in the region, including:

- **AI Lab (announced May 2018) –** a single flagship for Artificial Intelligence, machine learning and data science in defence based at Dstl in Porton Down. AI Lab will enhance and accelerate the UK's world-class capability in the application of AI-related technologies to defence and security challenges. Dstl currently delivers more than £20 million of research related to AI and this is forecast to grow significantly.[62]

- **Cheltenham Cyber Park:** Sited on the western fringe of the town, the entire development will occupy 135 hectares of land. Set on 45 hectares, the cyber park will deliver over 7,000 new jobs in 2m sq ft of commercial space, accommodate the larger corporation through to start-ups and SMEs, and also site the government's proposed cyber innovation centre, funded centrally. The park is intended as a concentrated site for the development of cyber security research, skills, business and capability in one geographical area. The project is overseen by a Strategic Partnership comprising the local authorities, the GFirst Local Economic Partnership, the Cheltenham Development Task Force, and supported by a number of government departments including GCHQ.

[62] GOV.UK, *Flagship AI Lab announced as Defence Secretary hosts first meet between British and American defence innovators*. Available at: https://www.gov.uk/government/news/flagship-ai-lab-announced-as-defence-secretary-hosts-first-meet-between-british-and-american-defence-innovators

4.4.3 Innovation Centres, Networks, and Research Organisations:

The region is home to a wide range of business parks, innovation centres, clusters and supporting infrastructure for businesses and cyber security research. These include:

Infrastructure:

- Skylon Park (Hereford Enterprise Zone)
- Malvern Hills Science Park
- Enigma Business Park
- Porton Science Park
- Wyche Innovation Centre (Key IQ)
- Ark Data Centre
- Berkeley C11 Cyber Security Centre
- The Kiln in Worcester (incubator space and support for entrepreneurial, innovating and scaling businesses across the area)

Supporting Networks, Clusters & Accreditation Bodies:
The region is home to several clusters, many of which are voluntary and passionate to share learning and grow the region's cyber security sector:

- **British Computer Society (Chartered Institute for IT): BCS,** The Chartered Institute for IT, promotes wider social and economic progress through the advancement of information technology science and practice. Founded in 1957, it has over 75,000 members globally. Whilst the BCS is a national body, it has a registered office within Swindon.
- **IASME Consortium:** one of only five companies appointed as Accreditation Bodies for assessing and certifying the Government's Cyber Essential Scheme.
- **Wayra (supplier delivering the GCHQ Cyber Accelerator):** As part of the UK's commitment to enhancing the UK cyber security capability, the accelerator has been set up to support new start-ups and cement their place in the growing UK cyber security ecosystem. The NCSC Cyber Accelerator is a collaboration between the UK Government Department for Digital, Culture, Media and Sport (DCMS), the Government Communications Headquarters (GCHQ), and Wayra UK, part of Telefónica Open Future. Wayra UK is a world-leading start-up accelerator programme, and provides coaching, support, mentoring, access to a dedicated accelerator facility, and the scheme also provides a financial grant of £25,000 to innovative cyber security firms.
- **Cynam (Cyber Cheltenham):** The goal of CyNam is to bring together the best technology minds from local SME's and start-ups to fully harness the rich cyber security ecosystem that flourishes around Cheltenham.
- **Cyber Security Clusters (UK Cyber Security Forum: Malvern / West of England)**
- **Corsham Institute:** an independent, not-for-profit organisation, based in Corsham and London. It provides insight and research into technology and data-driven services.

Strengths of our Infrastructure:

This section sets out a few examples of the infrastructure and space in the region which aims to incubate and grow the cyber security sector:

Skylon Park in Hereford is the designated Enterprise Zone of the Marches LEP. With a unique defence and security sector focus, building on Hereford's association with UK special forces as the home of the SAS, it offers a high-quality business space in a parkland setting.

The existence of other key sites, QinetiQ in Malvern and GCHQ in Cheltenham, form a local cluster of strategic sites from which Skylon Park draws. In total, defence and security businesses employ approximately 2,600 people across the Marches (ranging from manufacturers of military vehicles, weapons, explosives, systems and technologies, private security, security systems and investigation).

The 110-hectare site has undergone a multi-million investment in infrastructure, including site clearing, road building and the introduction of superfast broadband. Companies are invited to create their own place within the Masterplan of Skylon Park, giving flexibility for a space which best suits their operations in a central UK and European location. It is also within an hour and half drive of the international airports at Birmingham, Bristol and Cardiff. The site already benefits from the Rotherwas access road, giving the estate quick and easy access to the A49, M50 and the rest of the motorway network. To date 37 acres of land have been sold or developed in 21 separate sales/developments, with the sale of 26 further acres under negotiation. 41,500 sqm of workspace has been built, is under construction or committed to be built, with a further 20,000 sqm in the sales under negotiation. 38 businesses have moved onto the site including several defence and security businesses investing to grow their businesses.

There is an inevitable emergence of businesses in the security sector in Herefordshire. It is already the location for over 200 companies in the sector, many of which have been set up by ex-military personnel who have engaged in the Special Forces supply chain utilising their specialist skills to maximise business opportunities. Skylon Park is the only Enterprise Zone in the country to focus on the defence and security sector, aiming to build on the base of 70 plus small businesses operating locally in this market.

Skylon Park will be home to the Marches Centre for Cyber Security, due to open in 2020 (see Section 5.4.4).

Porton Science Park, is a new addition to the established Porton Science Campus which is home to DSTL and PHE Porton. It will provide new incubation and grow-on space totalling 3,950m2

The first phase of development at Porton Science Park has been funded by Wiltshire Council, the Local Growth Fund via the Swindon and Wiltshire Local Enterprise Partnership, and European Regional Development Funding.

Porton Science Park (PSP) provides an ideal location for companies working in the defence and security technologies, with close proximity to the Defence Science Technology Laboratory (Dstl)'s established expertise in defence science, engineering and cyber security, and to those companies based in the health and life sciences sector by benefiting from the existing world class expertise in the control of infectious disease, vaccinology and vaccine production facilities based at Porton and in the wider Wessex area.

Further development at the 10ha science park is strongly supported by the council and provides for larger developments for established companies seeking direct association with the Porton scientific community. The vision for PSP is to become a focus for innovation and market growth in its target sectors, through the provision of specialist services delivered in partnership with stakeholder organisations. A fully funded three year programme establishes a Health and Life Sciences Hub across the Swindon and Wiltshire area, based out of the PSP. Porton Science Park will support start-up business with:

- Dedicated business and venture management support, mentoring and advice
- Dissemination of knowledge and experience, with access to industry specialists
- Sector specific innovation support
- Networking and training opportunities
- Access to funding.

The Incubation Centre includes access to specialist equipment, technical expertise, collaborative research between businesses and the research community, and active linkages with existing innovation networks, higher education, and knowledge based industries, knowledge transfer networks and national and international knowledge bases. The Science Incubator has also been specified for a gigabit internet gateway for future occupiers.

PHE is in transition with a campus programme that will see significant elements of its science base relocate to Harlow in Essex by 2024. PHE will retain a presence on the Porton campus in the form of its regional Food, Water and Environment laboratory and a Cancer Registry, currently located in West Dean.

Malvern Hills Science Park – adjacent to QinetiQ in Malvern, the science park is home to a range of growing high-technology companies, many of which have 'spun out' of QinetiQ and have a specific Cyber Security focus.

QinetiQ is a significant industrial asset for the Worcestershire area. Based adjacent to the Malvern Hills Science Park, QinetiQ, formed from the privatisation of the Defence and Science Technology Laboratory, and prior to that the Telecommunications Research Agency, builds on a reputation of innovation and invention within the area (with significant developments in radar technology and the first touchscreen being developed in the area).

Over recent years small businesses spinning out of QinetiQ have formed a significant part of the Malvern Hills Science Park, and wider Worcestershire cyber cluster. Furthermore, QinetiQ has been a valuable strategic partner to the local partnership and has applied its expertise to a range of initiatives to help promote the profile and facilitate the growth of the cluster locally, and more widely across the region.

Enigma Business Park

"As an address, "Nimrod House, Enigma Business Park", seems particularly appropriate for a company [Deep-Secure] involved in encryption and secure communications for the British military" (FT, 2014)

Worcester is home to the Enigma Business Park, which houses Deep-Secure which provides network security guard services for assured information sharing. It has over 30 employees, and annual revenues in advance of £3m per annum.

Wyche Innovation Centre:

The Wyche Innovation Centre is home to the Malvern Cyber Security Cluster, in addition to Assure Technical, BlockMark, IASME Consortium, InnovaSec, and The Friendly Nerd. Its alumni have also included Surevine and Soteria. It offers business accelerator, technology incubation, and co-working space for cyber and technology start-ups.

Berkeley C11 Cyber Security Centre:

SGS Berkeley Green UTC is located at the Gloucestershire Science and Technology Park near Berkeley on a campus managed by South Gloucestershire and Stroud College in a £15m investment. The College has full-time Post 16 Engineering and Cyber provision on site. Within the same site at Berkeley, the University of Gloucestershire has also benefitted from a £3m growth deal investment to set up the **C11 Cyber Security Centre**. C11 provides a specialist "business-facing" cyber facility that includes secure conferencing, training, and testing and development space designed using industry standards. The C11 Centre is a joint initiative between the University of Gloucestershire (UoG) and South Gloucestershire and Stroud College (SGSC).

4.4.4 Future Significant Infrastructure Investments in Cyber Security in the Region:

This Audit has identified that across the LEPs, there is a strong commitment to promoting the cyber security sector and this is well reflected in upcoming infrastructure investments as summarised below.

Cheltenham Cyber Park: As previously set out, the cyber park will deliver over 7,000 new jobs in 2m sq. ft of commercial space, accommodate the larger corporation through to start-ups and SME's, and also site the government's proposed cyber innovation centre, funded centrally. The park is intended as a concentrated site for the development of cyber security research, skills, business and capability in one geographical area.

Marches Centre for Cyber Security: The Marches Local Enterprise Partnership (LEP) has successfully secured funding of £2.82m on behalf of the University of Wolverhampton from the Government's latest Growth Deal towards the cost of developing a new Centre for Cyber Security in Hereford**.** The proposed centre will form part of a 'Cyber Triangle' with GCHQ Cheltenham and the Government Cyber Centre in Newport.

Further investment plans include the £6.5m Shell Store Technology Incubation and Development Application Centre. This will provide 934 sqm of managed incubator space and 1,064 sqm space for students from the New Model in Technology and Engineering (NMITE) to interact with businesses on projects.

Skylon Park has designated a specific seven-acre site for a Cyber Campus. The centre piece will be its 2,700 m2, £9m Centre for Cyber Security, due to open by Spring 2020. The Centre, being developed by the University of Wolverhampton, will provide 3 elements:

- Offices/workshops/specialist laboratories for tenant cyber-related companies and incubation space for start-up companies (space for up to 16 companies)
- Advanced, secure facilities for the University and partners' cyber space research and development and commercialisation of intellectual property
- Secure training and educational facilities to provide specialist cyber security training for businesses and organisations

The building is designed and will be managed to provide users access to appropriate space, facilities, support, connections, knowledge and investment opportunities.

Over 3 acres of serviced, development ready land has been prepared alongside the Centre for related business development to accommodate either businesses growing from the Centre or other companies that want to be associated with and use the facilities of the Centre. Such companies will be able to exploit the focus, profile, opportunities and benefits that location on the Cyber Campus will bring.

The facilities will provide ready access to consultancy support from the University of Wolverhampton and provide shared facilities including lab space and training rooms. The combination of support, facilities and co-location with potential collaborators will significantly enhance the environment for investment and enterprise. It will contain specialist facilities for the

cyber sector including server space, very high-speed broadband, as well as R&D lab space. The physical fabric of the building will offer the high levels of security for data transmission and storage which will ensure Skylon Park attracts a growing base of cyber-related businesses and activity.

The building will provide users with access to space and support, connections, knowledge, experience and investment through:

- Over 1,000m² of R&D floor space for 3 cyber laboratories, providing new laboratory and testing facilities for researchers in this area.
- More than 1,500m² of employment space for 16 cyber security business incubator units, 2 workshops and 3 high security meeting rooms
- 250m² of high quality secure business training floor space

The fabric of the building will contain a physical security firewall between all major elements of the building and a secure server room.

The key partners in the development will be the University of Wolverhampton, Herefordshire Council and QinetiQ. The Centre will be a joint venture between the University of Wolverhampton and Herefordshire Council which will contribute the land on the Hereford Enterprise Zone for the development. The partnership with QinetiQ will allow the University access to an £80 million Cyber Range (one of only 6 in the UK), providing University researchers, students and businesses unprecedented access to sophisticated simulation and emulation cyber test-bed platforms.

Images of the Proposed Marches Centre for Cyber Security (due to open in 2020)

Corsham Mansion House

Corsham is integral to the Swindon and Wiltshire Local Enterprise Partnership's (SWLEP) Strategic Economic Plan and the emerging SWLEP Digital Strategy. Digital/Cyber and Information and Communication Technology is an important growth sector for the SWLEP with the potential to generate many high skilled, well paid jobs. The £2.5m LGF funding awarded for the Corsham Mansion House project will support incubating businesses with a digital outlook and help regenerate the local area. This business case applies HM Treasury Green Book Guidelines.

Corsham is home to a growing cluster of digital industries and a unique ICT infrastructure has built up around Corsham where the Ministry of Defence (MOD) and the private sector have invested heavily in secure communications and data storage. Economic Plan, and the Corsham Area Framework. The Corsham Mansion House project will build on these identified strengths and provide a facility that will incubate enterprises with a digital outlook. The Mansion House will nurture businesses, provide a collaborative working environment (including the scheduling of business events where the sector can come together to share ideas and network), and provide access to training and learning opportunities. In addition, the Mansion House can provide teaching space to enable the delivery of courses relating to the digital sector, and opportunities to engage with the industry, academia, institutions, the public sector and the public.

4.5 Local Science and Innovation Talent

4.5.1 Existing Talent

The digital economy, together with the cyber security sector is quickly expanding, and it is crucial to keep up with its growth by recruiting and developing the talent pipeline this requires.

In 2016, 85% of IT decision makers felt that there was a shortage of cyber skills in the UK and that by 2019 there would be a projected shortfall of 1.5 million cyber trained staff globally.[63] This equates to a training shortage of approximately 75,000 in the UK alone, and therefore within the Cyber Resilience Alliance, we recognise a need to train, upskill and encourage thousands of additional staff into the industry over the coming years.

A recent report from Indeed put the UK in second place globally in terms of demand for cyber-security professionals but only 12% of the cyber-security workforce are under the age of 35, indicating opportunity for an enhanced pipeline of talent coming into the industry where suitable training and skills can be deployed.

There are a wide range of initiatives and programmes in the Cyber Resilience Alliance region aimed to support talent into the sector, including but not limited to university and further education provision of courses, retraining and reskilling Initiatives, and Cyber Security Challenge.

Within the cyber security sector, it is also of real importance to recognise neuro-diversity and the need for an inclusive approach to finding new talent to address deemed skills shortages, which can be significantly alleviated where we work collectively to identify fresh solutions to meeting the market requirements.

4.5.2 Skills Gap

This section provides an overview of the key skills issues affecting the SIA area with regards to cyber skills. It examines vacancy and salary levels in the area, as well as skills gaps the area faces. It also examines best practice in the area, particularly around the addressing of these cyber skills gaps, and goes on to put the SIA area in context both nationally and internationally.

Data provided by IT Jobs Watch, an IT job market insight and analysis company, provides information on the number of job adverts and median salary offered for different IT jobs in the UK. *Table 4* shows the total number of job adverts that IT Jobs Watch has found in the cyber industry by geography. As shown, cyber security accounted for the largest number of vacancies in the SIA area with Gloucestershire accounting for nearly half (47%) of these.

[63] CSO Online, *Cybersecurity job market to suffer severe workforce shortage*. Available at: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html)

Table 4: Number of historical permanent job adverts in cyber jobs

	Cyber Threat	Cyber Threat Intelligence	Cyber Security	Cyber Essentials	Cyber Attack	Cyber Defence
Herefordshire	-	-	8	-	-	-
Malvern	-	2	13	-	-	-
Worcester	-	-	6	-	-	-
Worcestershire	-	2	26	-	-	-
Gloucestershire	7	10	115	3	5	1
Gloucester	5	5	19	-	-	-
Cheltenham	-	2	21	2	5	1
Swindon	8	-	10	-	3	-
Wiltshire	17	-	19	-	12	-
Stroud	-	-	1	-	-	-
Tewkesbury	-	-	30	-	-	-
SIA total	37	19	247	5	25	2
UK total	539	268	4,036	332	234	130
SIA as % of UK total	**7%**	**7%**	**6%**	**2%**	**11%**	**2%**

Source: IT Jobs Watch

According to ONS labour statistics[64], the SIA regions accounts for 3.9% of all jobs in the UK (across all sectors – 1.32 million of 34.06 million). For four of the six cyber sub-sectors listed in *Table 4*, the SIA's share of total vacancies is greater than 3.9%. This underlines the fact that in relative terms, the SIA region is a more important source of vacancies in the UK cyber industry than it is a source of employment across all sectors.

The SIA region appears to have particular strengths in the 'cyber-attack' sector where it accounted for 11% of all the vacancies posted nationally.

Table 5 shows the median salary for the cyber sub-sectors across the SIA area (where data are available). Public statistics show that the median earnings in the SIA region (across all sectors) are typically only 85% of the UK median wage.[65] Therefore, any instances where the local median wage is more than 85% of the national median for a given sector (as marked in red) will be indicative of wages that are untypically high.

[64] See SIA data dashboard prepared by Technopolis.
[65] Ibid.

As *Table 5* shows, there are many cases where the median wage is higher than might be expected. Indeed, there are several instances where the median wage is higher than the national wage, including cyber security in Herefordshire and Worcester respectively, and cyber essentials in Gloucestershire and Cheltenham respectively. This is in indicative of areas that are especially well-skilled in the cyber sectors, and/or where relevant labour is particularly scarce.

Table 5: Median salary for each sector for the 6 months to 25 April 2018 (where data are available)

	Cyber Threat	Cyber Threat Intelligence	Cyber Security	Cyber Essentials	Cyber Attack
Herefordshire	-	-	£59,500	-	-
Worcester	-	-	£82,500	-	-
Worcestershire	-	-	£50,000	-	-
Gloucestershire	-	£55,000	£45,000	£67,500	£28,987
Gloucester	-	-	£53,750	-	-
Cheltenham	-	£55,000	£46,250	£66,250	£28,987
Swindon	£48,750	-	£52,500	-	£51,500
Wiltshire	£47,500	-	£52,500	-	£47,500
Tewkesbury	-	-	£45,000	-	-
UK total	**£56,000**	**£60,000**	**£57,000**	**£57,500**	**£52,500**

Source: IT Jobs Watch. Figures in red represent median wages that are above 85% of the UK average.

Business organisations in the region have also commented on how they have faced cyber skills shortages. Business West for instance has described how many businesses in the region lack access to cyber security professionals who can help protect them from the ever-growing threats of cyber-attacks.[66] In 2017, *Gloucestershire Business Magazine* spoke about there being a more general digital skills gap facing Gloucestershire businesses.[67]

[66] Business West (2017) *Are we facing. Cyber security jobs recruitment crisis?* Internet, available at https://www.businesswest.co.uk/blog/are-we-facing-cyber-security-jobs-recruitment-crisis (accessed 1 May 2018)
[67] Gloucestershire Business Magazine (2017) *New apprenticeships bridging the IT skills*, p. 44. Internet, available at https://www.smarterwebcompany.co.uk/swbusiness-co-uk/_img/Glos_PDF_Gloucestershire_Business/Top%20100%202017_Gloucestershire_Businesses.pdf (accessed 1 May 2018)

4.5.3 Encouraging New Talent & Tackling the Skills Gap

The high wage levels, high job vacancy numbers, and cyber skills shortages mentioned above all point to a local cyber skills gap. Nevertheless, in recent times the SIA region has seen the introduction of a number of initiatives aimed at addressing this gap:

- **Cyber Schools Hubs:** linked to the National Cyber Security Centre (NCSC), Cleeve School in Cheltenham and Beauport Co-operative Academy in Gloucester have set up the UK's first Cyber Schools Hubs. Engaging with other schools in their area, the schools will host events, and trial new and innovative ways of introducing cyber security subjects to pupils. Local companies are also encouraged to be involved in the programme.[68]

- **National Cyber Skills Centre:** launched in April 2014, the National Cyber Skills Centre is a centre of excellence based in Malvern that is designed to "deliver high-quality, assured training provision to businesses and organisations to protect them against cyber-attacks."[69] Co-funded by Worcestershire County Council, the centre works with local and national training providers to help improve cyber skills within businesses.[70] It provides not only accredited courses but also leadership and operations training in cyber issues.
- **Cyber Security Challenge UK:** Cyber Security Challenge UK is a series of national competitions and learning programmes designed to inspire and enable more people to become cyber security professionals.[71] In 2016, it launched the UK's first Extended Project Qualification (EPQ) in cyber security. Equivalent to an AS level, the EPQ aims to gives students an understanding of the entire cyber domain, including risk management and digital forensics. Heart of Worcestershire College was chosen to develop a bespoke e-learning platform to enable delivery of the EPQ.
- **Cyber apprenticeships:** working in partnership with South Gloucestershire and Stroud college, Leonardo, an aerospace, defence and security company, in September 2017 became one of the first companies to offer a cyber apprenticeship. This scheme is targeted at students "who excel at GCSE or A-Level in IT-related subjects."[72]
- **Cyber security degrees:** both the University of Worcester and the University of Gloucestershire offer undergraduate degrees in cyber security. Working in conjunction with

[68] National Cyber Security Centre (2018) *UK's first Cyber Schools Hubs announced*. Internet, available at https://www.ncsc.gov.uk/news/uks-first-cyber-schools-hubs-announced (accessed 1 May 2018)
[69] Malvern Gazette (2014) *Centre of excellence launched in Cyber Valley, Malvern*. Internet, available at http://www.malverngazette.co.uk/news/11179680.Centre_of_excellence_launched_in_Cyber_Valley__Malvern/ (accessed 1 May 2018)
[70] Ibid.
[71] See https://www.cybersecuritychallenge.org.uk/about (accessed 1 May 2018)
[72] The Engineer (2018) *Engineering needs cyber security specialists to beat the threat*. Internet, available at https://www.theengineer.co.uk/355025-2/ (accessed 1 May 2018)

the Heart of Worcestershire College, the University of Worcester also offers a foundation degree in cyber security.[73]

- **Defence Academy of the United Kingdom:** Based at MOD Shrivenham just across the Wiltshire border, Defence Academy provides higher education for personnel in the MOD, wider government, UK industry and overseas. They have links to 11 universities and provide a wide range of courses ranging from awareness up to expert level covering five broad course themes: leadership; command; technology; business skills; and international engagement. In March 2018, the MoD announced the opening of a new Defence Cyber School at the Defence Academy, Shrivenham. Part of a joint investment by the MOD and the National Cyber Security Programme, the School will address specialist skills and wider education in line with National Cyber Security Strategy objectives.
- **The Cyber Club:** Completion of a successful pilot with the support of Gloucestershire Police has led to investment and a national rollout planned during late 2018. The Cyber Club is a trusted brand for organisations to access information about anything Cyber related. Aimed originally to be a low-cost solution for SMEs many public bodies and global organisation have joined. Current members include Barclays Bank, The FA Premier League, Mitie plc, Renishaw plc, Gloucestershire County Council, Clarkson Evans and HRH The Duke of York KG.
- **The National Cyber Awards 2018:** The very first is scheduled for November 2018 in Cheltenham with an emphasis onwards for Crime Prevention, Innovation including AI and Blockchain and recognition of unsung heroes particularly in the schools and charity sectors.
- **The Cyber Trust / Cyber 4Schools:** Chaired by Dame Janet Trotter DEBE CVO the Cyber Trust has been running a programme called Cyber4Schols that has attracted positive reviews across the UK. Featured on ITN News at 10 the charity seeks to expand its influence across the UK helping the vulnerable particularly around cyber bullying and coercion during 2019.

GCHQ CyberFirst: As a key part of the UK government's National Cyber Security Programme, CyberFirst delivers a broad range of activities designed to identify and support talented young people through their education and highlight exciting career opportunities in cyber security.

This includes courses, competitions, a thousand bursaries and the CyberFirst Degree Apprenticeship to encourage new talent into the sector. SANS, BT, FutureLearn and Cyber Security Challenge UK are partners to deliver the programme and prospective students, teachers, industry members and volunteers can now register their interest in advance of the scheme.

One of the initiatives recently organised by GCHQ was the CyberFirst Girls Competition in 2018. This involved 1,270 teams with over 4,500 girls (11-18 year olds) entering the 2018 competition. **The Cyber Resilience Alliance is home to three of the ten schools which reached the final** (Chipping Campden School, Gloucestershire, Pate's Grammar School, Gloucestershire, and St Augustine's Catholic College, Wiltshire).

[73] University of Worcester (date unknown) *Programme Specification for FdSc in Cyber Security*. Internet, available at https://www.worc.ac.uk/aqu/documents/FdScCyberSecurity.pdf (accessed 1 May 2018)

Across the UK, there is growing demand for cyber skills with the highest growth rates seen in Wales and the East Midlands. However, some 61% of advertised vacancies in the sector are in London and the South East, driven by the strong banking and tech industries there.[74] Even compared to other countries, the UK's demand for cyber skills is high. Analysis by Indeed indicates that the UK has the third highest level of demand for cyber security skills in the world with only Israel and Ireland seeing cyber security posting forming a larger share of total national postings.[75]

In order to service this demand, the UK is able to draw on a large talent pool. Although India and the United States together account for 32% of the world's cybersecurity talent (16% each), the UK has the world's third largest share of cybersecurity skills with 13% of the talent pool living in this country.[76]

However, this supply is not large enough to meet the current demand. Research from Indeed found that the number of people looking for cyber security jobs in Britain was just 31.6% of the total jobs posted in the area.[77] Shortages are especially acute in professions linked to spam, vulnerabilities associated with firms that have a Bring Your Own Device (BYOD) policy, advanced persistent threats (APTs), and spear-phishing.[78] This cyber skills gap is seen internationally as well as at a UK level. Israel for instance, has amongst the greatest demand for cyber skills in the world yet struggles to generate interest in relevant roles. As Table 6 below shows, jobs seeker interest in cybersecurity roles is amongst its lowest in Israel and the UK, but at its highest in the US and Canada.

Table 6: Interest in cyber security job postings across the world (Q3 2016)

Country	***Share of user clicks / share of cyber security job postings***
Israel	28.4%
UK	31.6%
Brazil	33.0%
Germany	35.0%
Italy	35.9%
France	38.6%

[74] Computer Weekly (2017) UK *cyber security workforce up to 163% in five years*. Internet, available at https://www.computerweekly.com/news/450412399/UK-cyber-security-workforce-up-163-in-five-years (accessed 1 May 2018)
[75] Indeed (2017) *Indeed Spotlight: The Global Cybersecurity Skills Gap*. Internet, available at http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/ (accessed 1 May 2018)
[76] Consultancy.UK (2018) *Majority of companies now hit by a cybersecurity skills gap*. Internet, available at https://www.consultancy.uk/news/16068/majority-of-companies-now-hit-by-a-cybersecurity-skills-gap (accessed 1 May 2018)
[77] Independent (2017) *A widening cyber-security skills gaps is threatening UK companies*. Internet, available at https://www.independent.co.uk/news/business/news/cyber-security-skills-gap-widen-supply-demand-expertise-uk-companies-it-a7529986.html (accessed 1 May 2018)
[78] Information Age (2017) *The cyber security skills gap in the UK: a multifaceted problem*. Internet, available at http://www.information-age.com/cyber-security-skills-gap-uk-multifaceted-problem-123466964/ (accessed 1 May 2018)

Country	Share of user clicks / share of cyber security job postings
Ireland	38.8%
Australia	42.3%
US	66.7%
Canada	68.1%

Source: Indeed

There is little of sign of this international skills gap ending in the near future. According to a Capgemini study, businesses worldwide believe that the demand of cyber talent will continue to rise in the short term. Their research, based on a survey of 1,200 senior executives and front-line employees from around the world found that 72% of respondents had predicted a high-point in demand for cybersecurity in 2020, compared to 68% today.[79] There is little sign that supply will keep pace with this growing demand. Analysis by PwC found that the cybersecurity workforce gap will widen to 1.5 million job openings worldwide in 2019, up from 1 million in 2016.[80]

Pictured: GFirst LEP Growth Hub

[79] per source 76
[80] PwC (2017) *Cybersecurity Talent Gap: Navigating the skills shortage*. Internet, available at https://www.pwc.com/us/en/cybersecurity/assets/pwc-cyber-talent-v3-v1.pdf (accessed 1 May 2018)

Case Study: Community Cyber Security Operations Centre: In aid of driving increased organisation security, a Cyber Security Operations Centre (SOC) is often an innovative and useful solution. A SOC is a centralised unit responsible for protection of an organisation's technology and software systems. It can serve many firms and can be attractive to local organisations wanting to secure their systems at a lower cost. In June 2018, a **Community Cyber SOC is established in Worcester to train neuro-diverse individuals in cyber security**, particularly those with an Autism Spectrum Condition, and to provide low cost internet protection for vulnerable groups.

The role of a community SOC is to further ensure that vulnerable members of society such as the elderly, people with learning disabilities and people who have already been victims of cyber-crime – are protected. The Community SOC will develop a methodology to provide chargeable internet protection services to vulnerable individuals, surrounding SMEs, schools and other organisations that struggle to afford traditional security services.

Only 16% of adults with Autism are in employment although many are highly capable. Many neurodiverse individuals have particular skills in being detailed, focused, and recognising changes in patterns. This often makes them especially talented in the field of cyber security. However, they find it difficult to work in a typical workplace due to their disability affecting their ability for social interaction, understanding workplace 'rules', and coping with noise and excessive activity.

This project will address the mental and economic disadvantages of neurodiverse individuals being in long term unemployment as well as addressing the growing skills gap in the cyber security market. The creation of a more diverse workforce in UK companies is also thought to make them more innovative and competitive in the long run which will benefit the UK economy.

The Community SOC will use QA online training, Immersive Labs platform training and in-person volunteer trainers to give neuro-diverse individuals a solid grounding and experience in cyber security. A training plan will be developed for each individual. This will include workplace skills as well as cyber security training. The project will be managed and delivered by IASME Consortium, and has received support from Aspie, Immersive Labs, DCMS, Titania, QA and many other local businesses signalling our commitment to finding and supporting untapped talent.

Case Study: Corsham Institute: Ci is working with a range of partners to test and evaluate different models for supporting people to move from unemployment to employment, or from one occupation or sector to another, through fresh or re-freshed tech and life skills training, which also address key tech and digital skills gaps regionally and nationally.

Its' Veterans Accelerator programme is delivered through SaluteMyJob, a social enterprise, and IBM's Corporate Citizen Programme. This classroom based course is hosted at Hartham Park, Corsham, where 150 veterans have gained certification in two of IBM's cyber security tools.

The programme has demonstrated that with technical training and life skills coaching and support, service leavers with a generalist background and no previous experience in tech, can successfully transition into well-paid jobs in the commercial cyber security sector. This proven model is now ready for further collaboration with employers across the South West and nationally to widen the pipeline into work; and for testing with other groups of people facing significant changes (ex-offenders and women returning to work, for example).

Corsham Institute is currently planning further initiatives to develop cyber security re-skilling and up-skilling learning opportunities across the region.

Further, the College @ Hartham Park is seeking to accelerate the build of a teaching facility and 350 seat auditorium as part of a planned capital investment programme. The traditional teaching facility will form part of a global network of HE, learning and enterprise capabilities for a through life education, training and skills programme encompassing digital, trust and security.

With the focus on trust, Digital and Secure-Tech, the education and skills development will be agile, responding to rapid changes in quantum, level and subject matter. Delivery will have measurable economic impact in SWLEP area and our collaboration with the best of breed HE Institutes and industry will have a local, national and international impact.

The College @ Hartham Park graduates will be creative problem solvers, thought leaders, understand the new and developing digital society and will be highly employable

4.5.4 Local Industrial Strengths and Capacities

The Cyber Resilience Alliance has a substantial and growing business base across cyber security and digital industries more widely. These businesses vary from large internationally recognised firms to smaller specialist start-ups and spin-outs. There are over eighty businesses identified within this Audit, however, the region also has a wide range of large firms beginning to develop and recruit in cyber security aligned activities, and an expanding range of start-ups and freelance cyber security experts.

The table below sets out the wide range of capacity and commercial strength within the region. Full case studies of some of the businesses in the region are included in Appendix G: Case Studies.

Worcestershire:
Vision Labs – a Kidderminster business as part of the Specsavers Group that uses machine-learning to develop face-recognition software for a variety of industries and applications, including security. **Titania** – An internationally recognized Worcester based Cyber Security business with multiple awards for innovation. Titania auditing solutions are deployed in over 90 countries and have unique capabilities in autonomous configuration auditing. They are key suppliers to the US DoD in the areas of Cyber Resilience & Vulnerability Identification, and Titania are facilitating the development of AI driven, fully autonomous self-healing networks. **QinetiQ** *(also active in Wiltshire)* – the UK's sixth largest defence contractor, employing over 2,000 individuals across a range of sites; with a substantial presence in Malvern on the site of the former national Defence Evaluation and Research Agency. QinetiQ work extensively on defence, cyber security and in related high-technology industries. **Deep Secure** – a supplier to leading intelligence agencies, defence departments and commercial enterprises. Deep Secure Ltd are a Content Threat Removal company that has recently been praised for its work addressing a gap in the market, through developing a platform that defeats known, unknown/zero-day and undetectable content threats without a need to understand or identify these threats. **Borwell** – Based at Malvern Hills Science Park, Borwell specialise in the development of tailor-made solutions that are 'Secure by Design'. The Borwell team supports several on-going MoD software projects for the RAF and Royal Navy, as well as working with NATO and the European Defence Agency (EDA). **BlackBerry Professional Cybersecurity Services (previously Encription UK):** Operating from a facility in Kidderminster, Worcestershire, BlackBerry operates a UK-based IT security arm that offers penetration testing, and IT security training courses for a mixture of public and private sector organisation. BlackBerry Cybersecurity Services was formed following

BlackBerry's acquisition of the Kidderminster-IT security and forensics services company, Encription UK. The new firm continues to offer services round strategic security (e.g. cloud services), technical security (e.g. IT infrastructure) and detection, testing and analysis. As outlined below, Encription has for several years, engaged with other stakeholders in the SIA area on issues concerning cyber security and resilience.

The IASME Consortium, based in Malvern, is a market leader in cyber security and governance certification. IASME is also one of the five companies nationally accredited to assess and certify against the Government's Cyber Essentials Scheme. The Cyber Essentials Scheme has been recognised as the best cyber security standard for small companies by the UK Government, and is a minimum requirement in bidding for some government contracts.

Gloucestershire

Raytheon UK: Raytheon unveiled its new £3 million cyber-crime fighting centre in Gloucester, England which is to house more than 100 of the UK's top cyber talent across big data, analytics and network defence. Further, Raytheon have a strategic partnership with the University of Gloucestershire providing bursaries to talented students and supporting the development of a degree apprenticeship in cyber security to close the skills gap in the region.[81]

BAE Systems Applied Intelligence – Based in Gloucester, BAE Systems Applied Intelligence provides security and resilience solutions.

Northrop Grumman: In 2015, Northrop Grumman, a global security firm, opened a new Cyber Centre facility with over 100 new jobs in Gloucestershire.

Cyberis – Based in Tewkesbury, Cyberis Ltd is an NCSC-approved CHECK company offering penetration testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures.

L3-TRL – Based in Tewkesbury, L3 TRL Technology is an agile UK-based company which designs, develops and delivers advanced electronic systems for the protection of people, infrastructure and assets. L3 TRL is part of the UK Cyber Growth Partnership. It has long-standing relationships with UK Government agencies and commercial service providers, developing award-winning IP encryption products that provide resilient protection of many sensitive and highly classified government networks.

IRM Security: Based in Cheltenham, IRM provide cyber consultancy services to support businesses meet compliance standards and mitigate risk. They also provide NCSC certified training courses and C-Suite briefings at a bespoke level through the IRM Academy. They support some of the UK's largest organisations, including Virgin Trains, the Post Office, GAME, and John Lewis.

Ripjar - Ripjar is a global company of talented technologists, data scientists and analysts designing products that will change the way criminal activities are detected and prevented. Its founders are experienced technologists & leaders from the heart of the UK security and

[81] University of Gloucestershire, available at: http://www.glos.ac.uk/news/Pages/university-and-raytheon-form-strategic-partnership-to-strengthen-cyber-security-capability-in-gloucestershire.aspx

intelligence community all previously working at Government Communications Headquarters (GCHQ).

3SDL is a leading defence and cyber data systems specialist, providing consultancy, services and training within the Defence and Security industry. Founded in 2005 and with headquarters in Malvern, cyber security is one 3SDL's core expertise with a team of specialists that support both government and business customers in identifying, prioritising, and addressing their cyber risks. Their services include threat assessments, design of technical solutions, cyber health checks, and the development of cyber security management plans including relevant training.

The company has engaged in a variety of collaborative activity with other cyber organisations in the SIA area. Working with other local cyber security firms, 3SDL is part of the membership organisation, Malvern Cyber Security Group. Consisting of around 40 other small cyber security firms, the members all co-operate with each other on initiatives to grow their businesses, to share practice, and improve cyber security. For instance, 3SDL worked with other Malvern-based companies Borwell, C2B2 and Deep Secure in developing a "dirty lab" research unit in Worcestershire to simulate attacks from hackers and have a secure environment in which to test virus counter-measures.

XQ Cyber – Based in Tewkesbury, XQ Cyber, an NCSC-approved CHECK company, that supports customers with advice and guidance; conducts laboratory and field research; and develops innovative solutions such as CyberScore, an affordable cyber security and third-party risk rating service.

PixelPin: PixelPin is a cyber-security company that was nominated as one of the most innovative mobile start-ups by UKTI and SMART in 2013. Its core product is a picture authentication solution that has been designed and built by world leaders in cybersecurity, working together to make the web safer for everyone. By eliminating the inherent weaknesses of the traditional text-based format, PixelPin offers a more secure and engaging way of logging into your accounts compared to traditional passwords. Its partners include KPMG and Microsoft, and it has received support from Digital Catapult, Wayra, L39 and the World Economic Forum. It is based in Cheltenham, with offices in London, New York and Tokyo.

Lockheed Martin (also based in Wiltshire)– a global aerospace, defence, security and advanced technologies company opened a £3m Cyber Security Centre in Gloucester in 2017. The 'Cyber Works' centre is designed to tackle cyber threats against the UK. The facility will create 90 jobs in Gloucester and enable Lockheed Martin to work with its UK partners to share knowledge, research and deliver 'cutting edge' capabilities.

Swindon & Wiltshire
Nationwide: Nationwide is the world's largest building society with over 15 million members. It is headquartered in Swindon, and its cyber security function is led here. In 2017, its head of Operational Risk was awarded an OBE for strengthening national cyber security.
Ark Data Centre: Corsham is home to one of Ark Data Centre's sites (Spring Park). This is a dedicated campus, comprises of 38 acres above ground, with access to 120 MVA diverse power supply, and has one million square feet of underground space available for development. It also has multiple fibre providers resulting in incredibly low latency (a fibre latency round trip to the City of London takes less than two milliseconds). The site is adjacent to secure MOD facilities and benefits from significant connectivity infrastructure. BT and the MoD are key clients of Ark Data Centres, and in 2015, Ark won a four-year contract with the Cabinet Office to supply the UK Government's hosting solutions (worth £700m).
Chipside: Chipside is a specialist software development company providing products and services to around a quarter of local and regional government traffic authorities in the UK. This means that Chipside works with over 130 local government authorities and throughout the UK, delivering smart city initiatives to villages, towns, and cities. These services include parking, real time smart city data gathering and reporting, and cashless parking permit systems. As a result of Chipside's innovation and market growth in recent years, the company is investing heavily in ensuring 'secure-by-design' methods and securing its data.
Intel Corporation: Swindon is home to Intel's main site in the United Kingdom and is one of the headquarters for its EMEA (Europe, Middle East, Africa) sales region. Intel's sales and marketing team in Swindon develops and deploys sound strategies to provide world-class sales and marketing support at the OEM, developer, and end-user levels. Additionally, Swindon hosts finance, HR, information technology, corporate relations, and other functions.
Foregenix: Foregenix are global leaders in digital forensics and information security. PFI, PFI Lite, PCI Compliance, P2PE, PA-DSS. Website and POS Security solutions. With their HQ in Marlborough (Wiltshire) they operate in the USA, South Africa, Uruguay, Germany and Australia. They offer high-level cyber security for businesses and develop software to uncover and prevent website security breaches. The company now employs over 100 staff despite only having 20 workers in 2014.
Torchlight: Torchlight is a global counter threat company. Torchlight provides a range of support to international institutions and organisations helping them better understand and mitigate complex and sensitive threats to their security and stability. They are the partner of choice for Information Security expertise across Government Departments and support the UK government and the EU with criminal justice development programmes overseas. Global contracts have helped drive sales to £10.1m this year.
Somerford Associates in Swindon provide security expertise to some of the UK's largest companies and can offer their products and services to Government Departments through G-Cloud. They work with innovative technologies that are disruptive to existing solutions, ensuring that solutions are robust, value for money, and are implemented quickly when compared to alternative solutions. Somerford are focused on enabling businesses to control

access to their data and help maximise the value of data to businesses. Solutions focus on Information Security, Cloud Solutions, GDPR, Internet of Things, Big Data.

The Marches

Anon AI: Based in Shrewsbury, Anon.AI provides automated data anonymization using AI. The product enables secure data sharing using a workflow tool that automatically anonymises and adapts to changing datasets. It is backed by CyLon (London based cyber security accelerator) and Post Urban Ventures (a Midlands-based start-up incubator).

Hex Security: Hex Security is an experienced Information Assurance consultancy based in Hereford. They are a certified provider of professional services by NCSC.

ZoVolt: Based in Hereford, ZoVolt (also known as Streembit) provides a decentralised peer-to-peer approach to communication and data sharing, providing scalable privacy without use of a central server.

XReach - Xreach is a leading supplier of highly secure communications solutions for businesses, government, military and security agencies. They provide situational awareness, and cyber assessment services.

Skylon Park in Hereford

4.6 National and International Engagement

The Cyber Resilience Alliance is outward-looking and recognises the potential to grow for significant sectoral growth will be generated through export-led initiatives. This section sets out some of the examples in how the region has engaged and promoted the sector nationally and internationally.

Examples of Engagement in the Region in Cyber Security:

Maryland
Maryland plays host to a number of US federal agencies, academic institutions and IT companies able to secure the U.S.'s infrastructure, with particular emphasis from federal agencies which play leading roles in delivering the nation's cyber security strategy.

- Maryland's top four research institutions conduct nearly US$1 billion of funded research annually combined.[82]
- Maryland's National Centres of Academic Excellence Research focus their research in network security, wireless systems, medical privacy and electronic voting, cryptography, intrusion detection, mobile and sensor networks and bioinformatics.[83]
- In 2016, the Midlands Engine Cyber mission took cyber security companies of all sizes from across the Midlands area to Baltimore, Maryland to attend the CyberMaryland Conference *(pictured below).*
- In return, during June 2017, companies from Maryland and the Midlands participated in a five-day Infosecurity Europe Conference in the Midlands, providing opportunity to share information and business opportunities.

[82] Maryland Department of Business & Economic Development. *CyberMaryland: Epicenter for Information Security and Innovation.* Available at: https://www.fbcinc.com/e/cybermdconference/default.aspx
[83] ibid

- In June 2018, Midlands Cyber coordinated a UK/US exhibition delegation to Infosecurity Europe 2018, Olympia London June 5-7, 2018. The exhibition is Europe's number one information security event, featuring the largest and most comprehensive conference programme with over 400 exhibitors showcasing the most relevant information security solutions and products to over 19,500 information security professionals.
- Maryland Department of Commerce led a US based delegation to the exhibition and co-located with Midlands Cyber to strengthen the two regions' Memorandum of Understanding (MOU) and showcase the innovative cyber companies from both Maryland and the Midlands.
- Drawing in more than 10,000 visitors, the event showcased local cyber security capability and the potential investment opportunities within the Midlands cyber sector.[84]
- Further to this, US and UK businesses met at two 'New Horizon' business events, in addition to a QinetiQ-hosted event. The relationship between the two regions has been cemented further with the signing of a Memorandum of Understanding, formalising their cyber partnership.[85]

"I'm delighted that we have signed a Memorandum of Understanding with Maryland, an internationally recognised cyber-security leader, with the world's largest concentrations of cyber security companies.

This builds on the successful CyberMaryland Conference in 2016 and a reciprocal visit earlier this month, where companies from across the Midlands and Maryland forged mutually beneficial partnerships. The MOU will further business development opportunities between the two regions and build relationships to grow our internationally-renowned cyber-locations."

Sir John Peace, Chair of the Midlands Engine

"[The] agreement with Midlands Engine will foster economic development, build our cybersecurity sectors, and spur economic growth in both the U.S. and the U.K. This exciting partnership will open up markets and opportunities for our cyber companies, allow cyber experts to share information and technologies, and further cement Maryland's standing as the cybersecurity capital of America."

Larry Hogan, US Governor of Maryland

[84] Worcestershire Local Enterprise Partnership, *US Delegation to Midlands Engine strengthens long-term business and academic partnerships*. Available at: http://www.wlep.co.uk/successful-us-delegation-midlands-engine-concludes/

[85] ibid

San Francisco

The RSA San Francisco exhibition is the world's largest cyber security conference, attracting more than 40,000 visitors, showcasing the talents of 700 cyber security exhibitors from across the globe.

- The Department for international Trade (DIT) brings eight first-time exhibitors to the RSA, providing a platform to demonstrate UK capability in cyber security, providing business and investment opportunity.
- The main offering for firms interested is a discounted rate to exhibit at RSA.[86]
- DIT will also offer UK pavilion companies investor introductions, network opportunities and US market briefings.[87].[88]

"The relationship between UK Government, regulators and industry has been integral in shaping the domestic cyber ecosystem. Having conducted significant research in this space, it is apparent that there is no other country or region that has the closeness of relationship between buyers, suppliers, government, regulators and academia."

Rowland Johnson, Chief Executive of Nettitude (Written Evidence to UK Parliament).

Israel

Israel has become something of a cybersecurity powerhouse, leading the way in an $82 billion industry.[89] It is identified as the sector giving Israel a global competitive advantage, based upon leading-edge research and unique practical applications experience.

The Midlands Cyber team visited Cyber Tech Israel, in Tel Aviv to raise awareness about the region as the UK's leading location for cyber expertise. The team met with several companies seeking the UK as a future market place for collaboration in sales and research.
The visit gave a great insight into the opportunity landscape for future projects for the region and what Israel can offer the Midlands in return. Israel is a hub of innovation, acceleration and the home to several incubators and R&D centres, populated with a plethora of future talent.

Another key component to Israel's rapid growth in the cyber space stems from the military background which serves to create both an accelerator and incubator environment for many start-ups, offering potential lessons and opportunities for the Midlands Engine given the concentration of UK military activity.

---

[86] Worcestershire Local Enterprise Partnership, *Cyber Security Trade Mission to RSA 2018*. Available at: http://www.wlep.co.uk/cyber-security-trade-mission-rsa-2018/
[87] ibid
[88] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/written/76741.html)
[89] https://www.midlandscyber.com/single-post/2018/02/08/Midlands-Cyber-Visits-Cyber-Tech-Israe

International Research:
The universities within the region are also developing several research collaborations internationally, which will help to cement the UK's place as a world-leader in cyber security knowledge transfer as well as provide commercial opportunities.

Within the University of Wolverhampton, joint research bids have been developed with the North Carolina State University, Georgia Institute of Technology, and Impacta College in Brazil. The current Memorandum of Understanding with Impacta College will help to develop the first MSc in Cyber Security in Brazil.

Further, the University of Gloucestershire also has a series of active relationships internationally and has worked with the Foreign and Commonwealth Office examining the role of Public-Private Partnerships in establishing cyber security strategy in Kenya, South Africa and Nigeria[90].

[90] University of Gloucestershire (2017) Towards Stronger Cyber Security PPPs in Developing countries, available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/FINAL%20REPORT%20CS%20PPP%20-%20FCO-BoE%20Final%20Copy.pdf

4.7 Developments in Technology

4.7.1 Introduction:

Cyber security is a business enabler, as it allows organisations to enhance and embed trust in their operations, which is conducive to improved innovation and trade. Where trust is compromised through a breach, organisations can suffer from not only material loss and theft, but also through reputational damage.

However, in the 'cat and mouse' game of cyber threats, those seeking to defend organisations from damage must continue to embrace technological innovation to prevent, defend and deter those undertaking attacks. The UK Government's Technology and Innovation Futures 2017[91] sets out four core reasons for public interest and the need for research and investment in emerging technologies:

- Potential **enablers of long-term economic growth** and productivity in the UK;
- Seeking the means to **improve the delivery of public services**;
- Identifying opportunities to **enrich the lives of our citizens**, as the internet has done, while **mitigating risks associated with technology**; and
- Informing **policy development** within government itself, particularly by **gathering better and more detailed evidence.**

The implications of technological innovation for the cyber security sector are far reaching. From a demand perspective, there is expected to be increased interest within emerging sectors including advanced manufacturing, autonomous and semi-autonomous vehicles, agri-food, and health and life sciences. Research by the RSA / YouGov (2017) has also highlighted that the majority of business leaders (76%) across the UK tend to agree that 'the introduction of new technologies tends to lead to increased cyber risks, which pose a significant threat' which ultimately requires the expertise of UK cyber security providers to help tackle and support trust in new technologies.'[92]

From a supply perspective, those providing cyber security products and solutions must respond to heightened and technical threats. As the National Cyber Security Centre has set out, 2017 was a challenging year for organisations seeking to secure their operations, with 'criminals launching more online attacks on UK businesses than ever before'.

> *"The last year has seen no deceleration in the tempo and volume of cyber incidents, as attackers devise new ways to harm businesses and citizens around the globe."*
>
> *Ciaran Martin, Head of the National Cyber Security Centre*

[91] Government Office for Science, *Technology and Innovation Futures 2017*. 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584219/technology-innovation-futures-2017.pdf

[92] RSA/YouGov Survey of 1,111 UK business leaders (April 2017) – Available in https://www.thersa.org/globalassets/pdfs/reports/rsa_the-age-of-automation-report.pdf

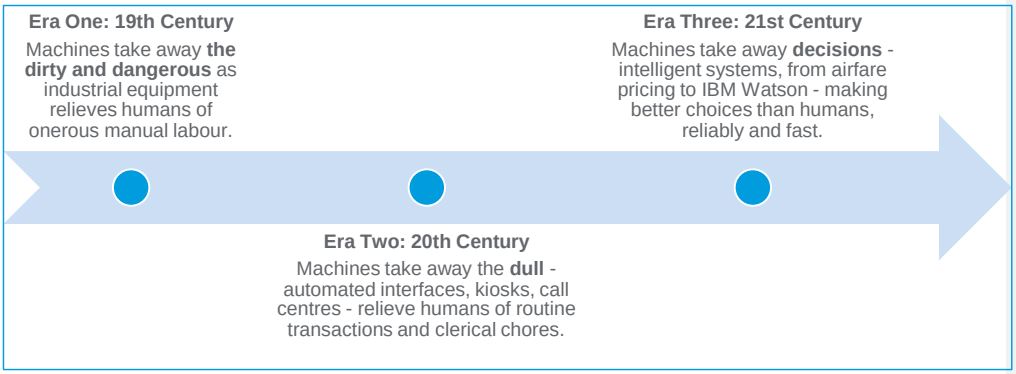
Where new emerging fields such as automation, Artificial Intelligence, and Machine Learning are being embedded into processes by industry, these are also becoming embraced by cyber attackers. For example, in 2018, the security firm Cybereason set up a fake server (known as a honeypot) to log all activities undertaken by attackers. It found that within seconds of going online, the server was quickly found and attacked by a bot which within 15 seconds had 'sought out and exploited several known vulnerabilities, scanned the network to which the server was connected, stole and dumped credentials and created new user accounts for its creators to use – all in an automated fashion undertaking 80% of the work a human might have previously undertaken'.[93]

Further, the proliferation in the number of Internet of Things (IoT) devices and increased business confidence in cloud computing also provides technical challenges for cyber security providers. For the Cyber Resilience Alliance, the following technology developments are of core importance to the cyber security sector: **Automation, Artificial Intelligence & Machine Learning, and the Internet of Things**. In recognition of the pace of technological innovation, the region will also further undertake technology foresight exercises regarding the sector, including the role of Big Data, Quantum Security, 5G, and how innovation in other sectors can align to the strengths inherent to the cyber security sector.

4.7.2 Automation

Automation refers to the use of control systems or workflows for operating equipment, running scripts and processes, or undertaking tasks with minimal or reduced need for human involvement within the processes. Whereas mechanisation refers to the effective replacement of human labour by machinery, automation implies the development of a self-governed process or system with digital integration and advancement in feedback loops.

Figure 16: 'Three Eras of Automation'



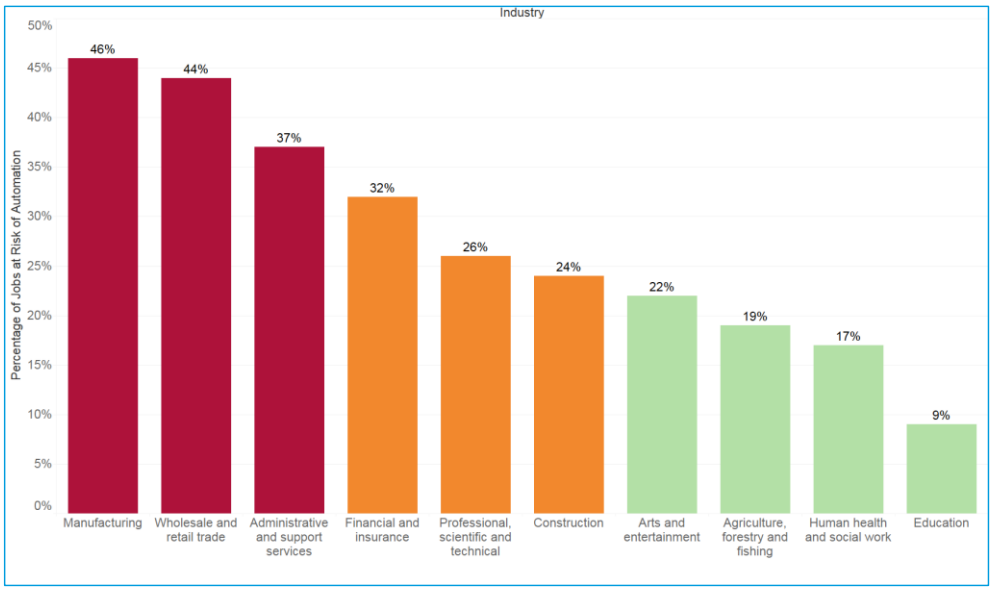
Source: Thomas Davenport and Julia Kirby from 'Beyond Automation' (June 2015)[94]

[93] BBC News, *'Lazy hackers' turn to automated attack tools*. Available at: http://www.bbc.co.uk/news/technology-43788337

[94] Harvard Business Review, *Beyond Automation.* 2015. Available at: https://hbr.org/2015/06/beyond-automation

Automation has been a key driver in public discourse regarding the future of work. Indeed, much of the discussion has focused on the negative impact of automation, including the potential for up to 30% of UK jobs considered at 'risk of automation by 2030'.[95]

Figure 17: 'Employment 'Risk' of Automation' (Source: PwC, 2017)



However, it is more likely that automation (as well as Artificial Intelligence, Machine Learning, and Robotics) will alter the employment landscape rather than lead to significant increases in unemployment and underemployment in the UK, given the wider potential for 'creative destruction'. Indeed, there is considerable potential for new jobs as a result of new technologies, including roles in designing, monitoring and repairing technology, engineering, machine learning and ultimately, supporting to ensure cyber security measures are in place.

[95] BBC News, *Robots to affect up to 30% of UK jobs, says PwC*. 2017. Available at: http://www.bbc.co.uk/news/business-39377353

As the Royal Society of Arts 'Age of Automation' (2017)[1]report has set out, the real implications of automation lie within its take-up and scale-up across UK businesses:

"New technologies could phase out mundane jobs, raise productivity levels, open up the door to higher wages, and allow workers to concentrate on more human-centric roles that are beyond the technical reach of machines. This is just as true for low-skilled workers as it is for high-skilled ones. But we cannot be complacent. AI and robotics, if deployed on a large scale, would result in both losers and winners. Some geographic areas, demographic groups, occupations and sectors would be hit harder than others. Economic inequality could rise, geographic disparities could deepen, and demographic biases could become further entrenched.

The challenge, then, is to accelerate… but in a way that delivers automation on our own terms."

Source: Royal Society of Arts 'Age of Automation' (2017)[96]

Automation in Cyber Security:
Automation within cyber security is fast becoming a core component of the offering from cyber security providers.[97] This may have significant implications for the cyber security sector, given strong employment and growth forecasts, and the potential therefore to automate some of the key roles of cyber security practitioners.

Consultations for this SIA indicated that there is growing consensus regarding the need for automation within the sector, given the expanding rate and pace of cyber attacks, in addition to the need to provide security solutions that do not require employing an unattainable or unrealistic number of cyber security specialists.

Whilst at present, many cyber security specialists spend considerable time identifying, analysing and responding to threats, these threats are evolving so fast that automated and intelligent defence layers deployed across an organisation's network that can autonomously identify threats and mitigate them are increasingly recognised as the solution.

Automation enables the ultimate creation of security solutions that can identify risk, threats and subsequently make decisions regarding monitoring, patching, quarantining and so on. However, as set out, automation also enables the pace and extent of attacks to increase, therefore the use of automated attacks calls for a similar solution.

[96] RSA, *The age of automation: Artificial Intelligence, robotics and the future of low-skilled work*. 2017. Available at: https://www.thersa.org/discover/publications-and-articles/reports/the-age-of-automation?utm_medium=referral&utm_source=Guardian&utm_campaign=age-of-automation&utm_content=report
[97] For example: http://www.symantec.com/controls-automation/; https://businessinsights.bitdefender.com/automation-ai-cybersecurity-skills-gap

Automation within the cyber security sector has been a recent phenomenon, it was only in the early 2010s, that the Defence Advanced Research Projects Agency (DARPA) in the United States observed sufficient developments in computer science necessary to automate the analysis and patching of software. In 2014, DARPA announced a competition to design and build computer systems that would block attacks or find and isolate malicious code. The subsequent winners could not compete with human cyber security experts, however demonstrated the pace of automation in cyber security within a short period of time.[98]

A number of large organisations have indicated their commitment to the role of automation in cyber security. For example, Microsoft announced in 2017 that it was buying the Israeli artificial intelligence cybersecurity firm Hexadite (for a reported $100 million)[99], it underscored the role of automation in addressing next-generation security threats.

However, automation should not be considered a process of replacement with few opportunities created in the process. A growing trend to emerge is the idea of 'cognitive assistants', in which systems interact with specialists to make their lives easier rather than replace them.[100] Analytics would be used to predict and screen threats with some automated corrective actions, whilst humans would then confirm threats and investigate. This process could support enhancements in productivity, with some of the more repetitive tasks automated.

Managing the workload share between automated programmes and human interventions will be extremely important for effective security. This shared workload will also mean the creation of new processes to manage interaction between the automated machine and cyber security experts, being able to identify, screen, and act on threats that clearly defines roles for smart machines and capable humans.

Anomali, in partnership with Phantom[101], provide a platform that delivers unified threat intelligence with security automation and orchestration. This enables the automation hundreds of security actions, incident backlogs and supports to 'shrink the gap between cyber security need and capability'. In their view, organisations lack the skilled professionals required to analyse the volume of incidents that occur daily, leaving the majority of alerts un-investigated as cyberattacks continue to grow in frequency and magnitude. The combined solution automates repetitive tasks, allowing security teams to focus their attention on the most mission-critical decisions in their organisation. By automatically delivering Indicators of Compromise (IOCs) from the ThreatStream Platform to the Phantom Platform, the combined solution automates hunting, investigation, alerting, and response -- giving time back to analysts otherwise spent completing the tasks themselves.

[98] The New York Times, *Automating Cybersecurity*. 2014. Available at: https://www.nytimes.com/2014/06/03/science/automating-cybersecurity.html
[99] TechCrunch, *Microsoft to buy Israeli security firm Hexadite, sources say for $100M*. 2017. Available at: https://techcrunch.com/2017/06/08/microsoft-confirms-its-acquired-hexadite-sources-say-for-100m/
[100] ComputerWeekly.com, *IBM cognitive assistant to help manage and secure devices.* 2017. Available at: https://www.computerweekly.com/news/450415135/IBM-cognitive-assistant-to-help-manage-and-secure-devices
[101] Anomali, *Anomali, Phantom Partnership Provides Cybersecurity Automation and Orchestration*. 2017. Available at: https://www.anomali.com/news-events/press/anomali-phantom-partnership-provides-cybersecurity-automation-and-orchestration

Ultimately, the emergence of IoT, and the wider proliferation in devices and connectivity means that cyber security systems reliant on human input are unlikely to be resilient in the years to come. Automation is increasingly becoming a focal development within the cyber security industry; however, it is likely that there is still a need for human input to guide its deployment. Within the backdrop of labour challenges and skills gaps in the cyber security market, automation offers a compelling case for investment and further research and development.

Cyber Resilience Alliance: Leading Automation

There are many firms within the Cyber Resilience Alliance which have embedded principles of automation into their product development. Further, automation will likely play a key role in the growth of the wider region's economy (in automotive and autonomous vehicles, manufacturing, and agri-food), and it will be crucial to secure these technological gains by default.

Titania, a cyber-security automation firm based in Worcester, is a world leader in the automation of configuration analysis to enable autonomous Network and Endpoint hardening.

By drawing upon, replicating and automating core penetration testing expertise in its Network and Endpoint auditing solutions, Titania have created automation tools which not only provide unrivalled automation accuracy and flexibility - they help close the skills gap.
Recognising that Cyber Hygiene (taking care of the Cyber basics) and scarce human resources remain two fundamental challenges across the Cyber Industry generally, Titania's software replicates the work of security consultants – freeing them up from essential but mundane work. Their solutions deliver increased visibility of vulnerabilities, remove many of the false positives and negatives that create SOC Alert Fatigue and improve response and resolution times while addressing Cyber Hygiene issues at scale.

Titania is working with Government and Industry to leverage its intelligent virtual modelling technology to deliver Enterprise wide, prioritised continuous diagnostics and monitoring as the best of breed Configuration Analysis component of Security Operations Centres (SOC). This has resulted in large scale deployments and close collaboration with Cyber Leaders within US Government (DOD/Federal) and UK Government UK (MOD/Civil), as well as world leading Enterprises in Aviation, Financial Services, Retail, Telecommunications and Utilities.
Clients include Military, Civil/Federal and Enterprise customers in approx. 90 countries worldwide saving thousands of man-years every year.

Tanium (US firm, with offices in Cheltenham) has also been involved in integrating automation into their capabilities. Tanium is a platform that provides 15 second visibility across all endpoints, even in large organisations. The platform can be used to search for varying IOC formats, monitor for anomalous behaviour, patch endpoints, monitor configurations, discover unmanaged assets, or investigate and respond to an incident. The speed and simplicity of the platform also enables small teams to be more efficient, by more quickly gaining access to required information, automating key tasks, and spending less time supporting a complex architecture associated with typical hub and spoke architecture. The available API and ability to develop new content, also allows organisations to integrate the platform with existing processes and other point solutions.

4.7.3 Artificial Intelligence[102] [103]& Machine Learning

"There is no doubt that machine learning and AI is already improving peoples' lives, from intelligent personal assistants that can prepare us for changes in the weather, to systems that protect our money from criminals, or devices that offer medical advice from the comfort of our own home. And this is only the start; the potential of AI is undeniable. Our next challenge will be to harness this technology to transform how we diagnose diseases, manufacture goods and build our homes. Using advanced algorithmic techniques such as 'deep learning', AI has the potential to solve complex problems fast, and in so doing, free up time and raise productivity."

AI Sector Deal, HM Government 2018

"Cyber security is a good example of an established digital sector that will see an improvement in performance with greater use of AI. A large number of organisations face cyber threats every day. ***Machine learning can identify, categorize and analyse these more effectively than individual researchers****. By working simultaneously on different tasks, across a large number of devices and systems,* ***AI can help defend against large attacks****. Automating some cybersecurity functions can help identify anomalous behaviour more quickly, highlight areas of concern that can be followed up by human network engineers, and identify and patch network weaknesses before they are exploited."*

Growing the Artificial Intelligence Industry in the UK (2017)

Introduction:

It is estimated there are approximately 200 firms across the UK currently developing AI products in the UK, including within cyber security (Darktrace in particular). Research by Asgard (2017) has found that the UK has Europe's strongest AI ecosystem.[104] It has been estimated that AI could add an additional USD $814 billion (£630bn) to the UK economy by 2035, increasing the annual growth rate of GVA from 2.5 to 3.9%.

Machine learning refers to systems that can automatically improve through experience. Machine Learning software gains the ability to learn through observation that makes assumptions and inferences about future behaviour. Machine learning is a natural fit for cyber defence and malware scanning. Indeed, historically, antivirus software has been signature-based, meaning

[102] GOV.UK, *AI Sector Deal.* 2018. Available at: https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal

[103] Hall, D.W. and Pesenti, J., 2017. Growing the artificial intelligence industry in the UK. Report, HM Government, London, United Kingdom. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

[104] Asgard, *The European Artificial Intelligence Landscape | More than 400 AI Companies Built in Europe.* 2017. Available at:https://asgard.vc/the-european-artificial-intelligence-landscape-more-than-400-ai-companies-made-in-europe/

that security companies identify specific malicious programs, extract a sort of unique fingerprint for each of them, and then monitor customer devices to ensure that none of those signatures appear.[105]

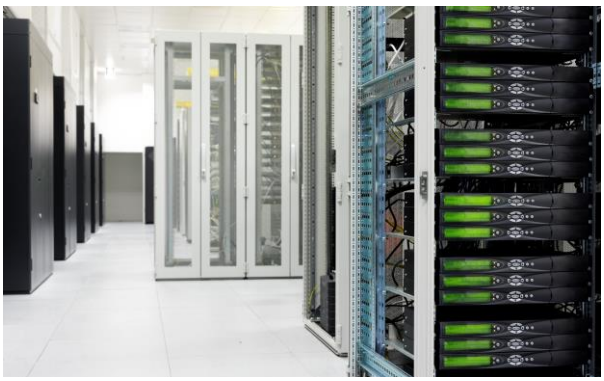
The general use of machine learning for cyber security can be summarised as seeking out anomalies. It can be used to identify malicious behaviour and entities. Machine learning has been utilised by organisations across several tasks and practices to reduce the impact of cyber-attacks. Machine learning tasks typically include regression (prediction), classification, clusterisation, recommendation and reinforcement. Cyber Security tasks are often put into the following categories that have some overlap with the capabilities of machine learning: prediction, prevention detection, response and monitoring, and machine learning is often used for technology layers such as network traffic analysis, intrusion detection, anti-malware, database firewalls and anti-fraud.

Regional Strength: Ark Data Centres:

"The algorithms that have driven much of this success depend on an approach called deep learning, which uses neural networks. Deep learning algorithms have a significant advantage over earlier generations of ML algorithms: They can make better use of much larger data sets. The old systems would improve as the number of examples in the training data grew, but only up to a point, after which additional data didn't lead to better predictions."

According to Andrew Ng: More data leads to better and better predictions. Some very large systems are trained by using 36 million examples or more. **Of course, working with extremely large data sets requires more and more processing power, which is one reason the very big systems are often run on supercomputers or specialized computer architectures."**

Source: HBR (2017) 'What's Driving the Machine Learning Explosion?"



4.7.4 Internet of Things (IoT)

Internet of Things (IoT) combines advanced analytics and a plethora of devices that connect together by communication technologies which allow for monitoring, collection, exchange and analysis of data of these devices to deliver valuable insights. IoT allows companies to build a data footprint through sensors and monitoring of equipment and machinery. This will enable new business models which provides greater opportunities for the cyber security sector to work closer with industry.[106] [107]:

Economic Potential of IoT

- The IoT is predicted to generate up to $11 trillion in value for the global economy by 2025.
- The IoT will bring 67,000 jobs to the UK by 2020.
- Adopting the IoT on an industrial level (the IIoT) could boost the UK economy by £352 billion by 2030 (Accenture).

IoT can only be utilised to its full advantage with adequate digital infrastructure, including Low Powered Wide Area Networks (LPWAN) and 5G to facilitate the sheer scale of data exchange, and enable real-time monitoring and connectivity between devices.

"Autonomous systems are a juicy target for cyber criminals and we need to assure ourselves that they are safe to use from a cyber perspective otherwise the market will fail." Director of a Cyber Resilience Alliance SME

With the proliferation in IoT devices, there is an increased need to ensure that manufactures of devices adhere to agreed standards regarding device security to prevent creation of botnets or device-based vulnerabilities.

As set out by the Made Smarter Review (2017), 'the risk of this on a global scale is almost unquantifiable as it can impact reputation, relationships with a broad range of customers and partners across the supply chain - not to mention production, logistics and (as manufacturing begins to develop a closer relationship with consumers) personal data. During the WannaCry ransomware attack earlier this year, manufacturing businesses such as France's Renault were affected which led to them temporarily stopping production at several sites to prevent the spread of the attack'

[106] GE Digital, *everything you need to know about the Industrial Internet of Things*. Available at: http://invent.ge/2eqfX43

[107] Department for Business, Energy, & Industrial Strategy, *Made Smarter Review 2017*. 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655570/20171027_MadeSmarter_FINAL_DIGITAL.pdf

UK IoT:
The UK is home to a rapidly growing community of companies developing and commercialising IoT component technologies, products and services. The UK government has invested significantly in the connected technologies sector through the £32 million of funding awarded to the IoTUK programme in the 2015 Budget.

IoTUK is a national initiative designed to support IoT development and uptake in the UK, through applied research, demonstrating the technology at scale, attracting international investment and supporting small companies.

Underpinning the success of IoT in the UK will be ensuring trust and security, and provision of the infrastructure to best support the sheer scale of connectivity between devices.

Technological Advantage in the Cyber Resilience Alliance: 5G Test Bed

Worcestershire LEP and key partners have been awarded grant funding from the Department of Digital, Culture, Media and Sport to develop a 5G Test Bed that will support the development of commercial 5G applications.

In its first phase, local businesses such as Worcester Bosch, Yamazaki Mazak, and QinetiQ will use the 5G Test Bed to develop initiatives focused around Industry 4.0 and Remote Manufacturing, and the applications of these technologies to increase productivity and support the development of future-proofed cyber security services. In the second phase of the 5G Test Bed, further businesses will be able to pilot their commercial products using 5G technologies.

Companies at Malvern Hills Science Park will trial the technology before it is made public, with defence technology company QinetiQ using it to test advanced cyber security applications.

"*Worcestershire LEP has demonstrated very advanced vision in its drive to be leading centre for the use of 5G in Industry 4.0 factory automation, Cybersecurity Applications, Robotics and Agritech. The 5GIC is very pleased indeed to be a partner in this exciting proposal, which we believe is world class. We are particularly excited by the opportunity this will provide to engage the international telecommunications companies, which are members of 5GIC."*

Prof Rahim Tafazolli, Director of the 5G Innovation Centre

4.7.5 Sector Potential for the Region:

Based upon the technological developments and the strengths of the region, there are a number of sectors within the region where cyber resilience and cyber security products can be embedded to improve overarching productivity and value-added.

These include (but are not limited to):

Agrifood & Agri-Tech:

- The economy of Shropshire, Herefordshire and the Marches has a particular focus on agriculture. 85% of land in Shropshire and 84% of land in Herefordshire is devoted to agriculture and over 6,300 farm holdings across the Marches area. The region has more people employed in Agri-Tech than any other LEP area.

- Harper Adams University is a key asset for the Agri-Tech industry in the Marches. It is the leading UK institution specialising in agriculture and agricultural engineering, as well as being an internationally recognised Centre of Excellence in this sector.

- Nearby Keele University, in our neighbouring LEP, offers a complementary Sustainability Hub. In 2016, it received a share of £1.7 million[108] in government funding to run two new engineering conversion courses, specifically in Automotive Engineering and Agricultural Engineering. This is part of a broader drive to develop engineers to meet the future needs of employers, which include 'data science, cybersecurity, and software engineering'.

Autonomous Vehicles:

- Autonomous vehicles are a key area of growth that could be vulnerable to cyber security issues. These are vehicles that can sense the environment and navigate without (or with limited) human input. These operate using radar, laser light, GPS, odometry and computer vision.
- Jaguar Land Rover has considerable presence adjacent to the SIA region. Five of their six UK locations are based in the West-Midlands which include in Birmingham, Coventry,

[108] Harper Adams University, Harper *Adams receives share of £1.7m to start engineering conversion courses*. 2016. Available at: https://www.harper-adams.ac.uk/news/202805/harper-adams-receives-share-of-17m-to-start-engineering-conversion-courses

and Wolverhampton. The Wolverhampton location is the only location to be situated within the SIA however. UK Jaguar Land Rover's Wolverhampton base, The Engine Manufacturing Centre, was opened in 2013 and employs nearly 1,400 people.

- Jaguar Land Rover have announced plans to help in the production of self-driving cars, and will create a fleet of more than 100 research vehicles over the next four years.
- The Government wants to build new experimental roads in the West Midlands which are designed specifically for driverless cars. This was revealed in the Government's Industrial Strategy and is part of a plan to see UK companies at the forefront of autonomous vehicles. £150 million is available for firms, including JLR, to test autonomous vehicles on public roads by 2021. A £5m trial to test 5G applications. and deployment on roads in 2018, will help to test how we can maximise future productivity benefits from self-driving cars, building on the work already progressing on connected and autonomous vehicle trials in the West Midlands. The first of Jaguar Land Rover's fleet of over 100 research cars will be driven on a new 41-mile test route on motorways and urban roads around Coventry and Solihull throughout 2016. With the increase in use and investment in autonomous vehicles comes with it greater risks of cyber security threats, especially given the nature of how autonomous vehicles function

Advanced Manufacturing:

- The scope of Advanced Manufacturing covers opportunities for research, development, prototyping and practical application in the areas of Advanced Materials, Innovation and Vehicles. The University of Wolverhampton's Telford Innovation Campus, located next to the main business parks of Telford, currently houses: Research; Business Engagement; Process & Product Development; Education; CPD and training activities. It is home to 300 students studying engineering-based courses as well as approximately 50 businesses. Approximately £12m is currently being invested in the campus to create new state-of-the-art facilities and courses to help create the next generation of skilled engineers in response to the regional and national shortage of engineering graduates.
- Worcestershire has an automotive supply chain, linking with Jaguar Land Rover and other car manufacturers.[109] Machine manufacturing and engineering employment is approximately 85% above the England average per capita. It is home to Yamazaki Mazak, the world's largest producer of computer-controlled metal cutting machine tools, encompassing everything from jewellery to jet engines. The company's European Head-quarters and its UK base are in Worcester, which houses one of the most advanced manufacturing plants in Europe and employs over 400 people.
- Adjacent to the region, The University of Birmingham has an Advanced Manufacturing Technology Centre, with key partner Rolls Royce, and this specialises in practical applications, manufacturing development, problem solving and improving competitiveness.

[109] Worcestershire Local Enterprise Partnership, *Advanced* Manufacturing. Available at: http://www.wlep.co.uk/about/worcestershire/about-wlep/growth-sectors/advanced-manufacturing/

4.8 Developments in the wider funding landscape

The cyber security sector has been visibly supported by the development of the National Cyber Security Strategy (2016-21) with its flagship investment of £1.9bn in UK cyber security over five years.

However, this reflects one fund among many in an active sector with several routes to support scaling, growing and breaking down barriers to entry and growth for cyber security firms. This section provides a broad overview of the funding and support available to firms, evidencing the potential sources for public and private support.

The Cyber Resilience Alliance will identify potential funding streams to enable collaborative projects with regional, national and international bodies to best maximise the funding available in the UK to grow the cyber security sector, and to support firms and organisations become more cyber resilient.

(See Appendix I: Funding for further detail into the funding landscape)

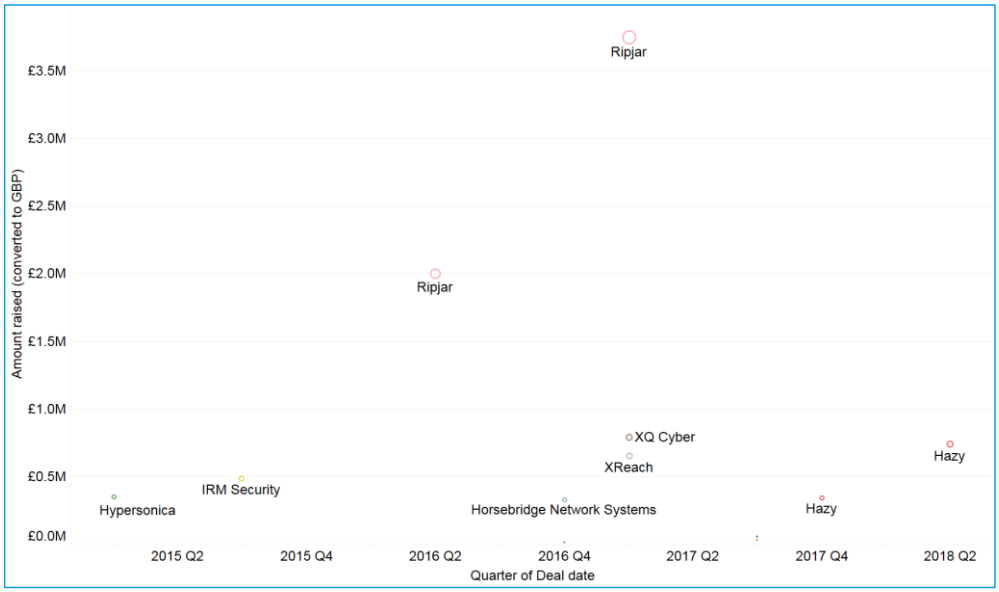
4.8.1 Analysis of Venture Capital Investment:

Within the SIA, a total of £9.5m was raised by 'digital security' firms in Venture Capital investment between Q1 2015- Q2 2018. There were 12 investments in the region.

In the same period, the UK's 'digital security' firms raised £1.28bn in VC, across 393 investments.

The SIA represents 0.7% of UK Venture Capital Investment in Cyber Security, and 3% of the Investments. The largest investment received was by Ripjar (£3.8m in Q1 17). This suggests that the larger scale investments in cyber security are taking place outside of the region (e.g. London), and that investment in the region is focused upon innovative start-ups.

Fig 18: VC Investments in the Cyber Resilience Alliance (in Digital Security)



Source: Beauhurst

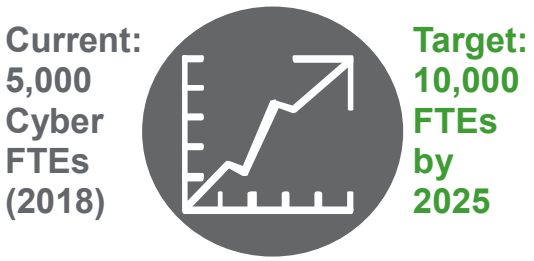
5. CONCLUSIONS

5.1 Vision:

To maximise the opportunities of the cyber security sector in the Cyber Resilience Alliance, we set out the following evidence informed vision for the region.

Firstly, we want to double the size (measured by employment) of the cyber security sector in the region, aligning the potential of our people with high-value employment into firms that can be global leaders.

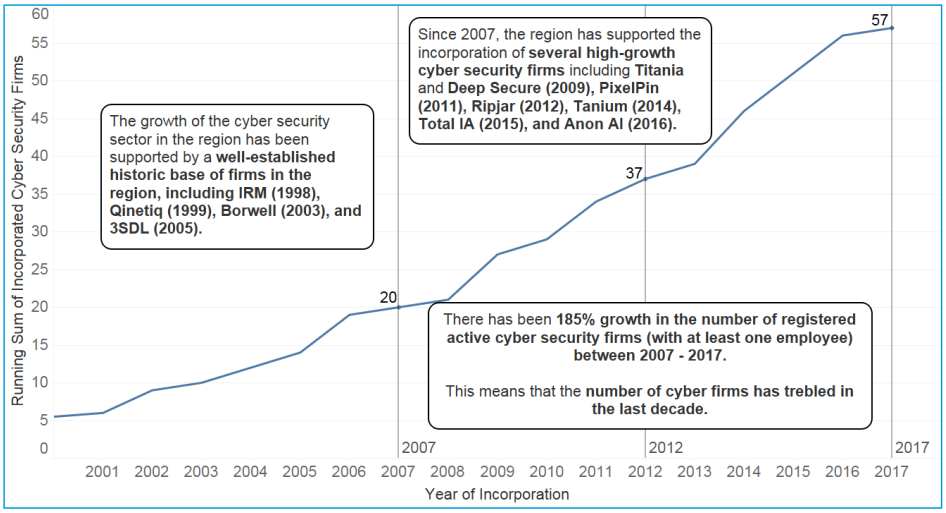
We will plan interventions in line with anticipated and sustainable growth (approximately 10% per annum).



By 2025, we aim to have 10,000 (FTEs[110]) employed in the sector.[111]

Secondly, this Science and Innovation Audit has confirmed many of the propositions set out within our Expression of Interest: the region is particularly strong in cyber security with respect to the number of firms (more than fifty cyber security firms[112]), and over a hundred organisations and firms actively shaping cyber security products, services and development. As a result, we want the region to be known nationally and internationally as the **UK's largest cluster of cyber security activity outside London.**

Registered Cyber Security Companies within the Region: A Rapidly Growing Sector…



Source: Bureau van Dijk

[110] Full Time Equivalent staff
[111] See Section 5.3 Employment Estimates and Projections
[112] DIT (2018) Cyber Security Export Strategy identifies c. 800 cyber security firms in the UK.

Thirdly, with this recognition, we want to ensure that the region continues to promote an entrepreneurial start-up culture & attracts new investment. As a result, by 2025, we estimate that the region's sector will contain more than one hundred active cyber security firms – and with further investment and support, this figure could be even higher particularly given the attractiveness of the region (competitive operational costs for business, a growing talent pool, and strong clusters of cyber innovation). Further, we will endeavour to identify opportunities for firms in manufacturing, defence, automotive, financial services and other sectors to embrace cyber security as a core component in product development.

This aligns to the findings of this Audit that nominal R&D expenditure has increased within the West Midlands and South West since 2008 at twice the national rate (grown 43% between 2008-14 compared to 21% across the UK). In recognition of the rapid growth in BERD[113] in the region, and the potential for disruptive technologies to require cyber security solutions (particularly in advanced manufacturing and automotive), we will support cyber security firms to identify UK supply chain opportunities that can further grow R&D expenditure in the region, improving the quality and value of our strong manufacturing base.

Finally, we recognise there is a long-standing productivity gap in the region. GVA per capita in the region is £22,804 (2015). This means that productivity is 10% lower than the UK's GVA per capita (£25,351). Tech Nation (2017) identify an average advertised digital salary of £36,236 in Worcester and Malvern. Further, there is also a nationally recognised 'cyber dividend' with regard to salaries. Technopolis analysis indicates that in the last six months of 2017, median advertised salaries in cyber security in the region ranged from £45,000 (Tewkesbury) to £82,500 (Worcester) – with a national median of £57,000 per annum.

With regard to productivity and earnings, there is clear potential for growth in the cyber security sector to improve the region's GVA per capita, and support efforts to narrow the productivity gap over the next decade.

Further, the Audit set out to explore how the expertise within the region could be utilised to best develop talent and embed cyber resilience within firms across industries. There are strong initiatives in the region to achieve these aims, including (but not limited to) the Cyber Club, the Malvern and West of England Cyber Security clusters, and the IASME consortium[114]. Our vision for the region is to embed cyber resilience through the promotion of initiatives that encourage wider investment in cyber security products and processes across all industries.

Long-term, it is our ambition that the Cyber Resilience Alliance Region is recognised as a world-leading cluster, and there are many opportunities for our businesses and organisations to embed and promote cyber resilience globally, and to lead within cyber security export markets.

[113] Business Expenditure on Research & Development, See Section 4.2 Research Strengths and 4.3 Innovation Strengths and Growth Points
[114] See Section 5.5 Local Science and Innovation Talent

5.2 Gap Analysis:

Whilst the cyber security sector has demonstrated rapid expansion and growth in the region in recent years, there remain gaps that are restricting the growth and potential of the sector, and present challenges for the future sustainability and talent flow in the industry.

Within cyber security, these gaps impact not only the sector directly, but impact the UK's capacity to defend its national infrastructure and provide an adequate cyber response function regarding national security. Within the region, given the concentrated presence of cyber security businesses and critical national infrastructure, there is a fundamental need to address these gaps and to ensure a sustainable model for the growth of UK cyber security.

This audit has identified the following core gaps that must be considered in future interventions to support the sector within the region.

5.2.1 Development of Skills & Talent:

Several of the SME cyber security firms in the region consulted throughout this Audit process highlighted the significant gap in the region regarding a skills shortage. As reflected in Section 5.4, there are hundreds of unfilled vacancies in the region within cyber security. This is for several reasons, including:

- The perception that the City of London has the 'pull' to attract some of the nation's best talent, leaving other parts of the UK with more limited potential for recruitment. This highlights the need to showcase the Cyber Resilience Alliance region as attractive to live and work in;
- A perceived gap within the skills accredited (Level 7+) and the applied and commercial skills required by businesses;
- Demand for labour considerably exceeds supply: this is creating a labour market with salary costs potentially prohibitive to new innovative start-ups (e.g. salaries in the region of £50,000+ for staff with one to two years' experience);
- The current provision of skills and talent (formal university / higher education, and conversion courses and training schemes) offers a strong model to address many of these gaps, with the Universities of Gloucestershire, Worcester and Wolverhampton taking welcome steps to grow the talent pipeline; however, given the sector's strong growth, there is a gap between what is needed and what can be produced.

> *"Talent is the largest single limiting factor to the growth of UK cyber security companies and the market. Low talent concentration leads to inflated salary costs and provides a barrier of entry for new innovative start-ups."*
> *(Worcestershire – large cyber security firm)*

Consultees did note, however, that the Cyber Resilience Alliance region is not the only cyber security cluster fighting for cyber security specialists, commenting on the need for the region to vie with talent across the entire UK.

5.2.2 Provision of Facilities and Infrastructure: Reflect the Breadth & Diversity of the Sector:

This Audit has identified the wide range of funding and infrastructure initiatives across the region and wider UK for cyber security.

The region is host to several of the UK's leading examples of cyber security incubation and acceleration including the Wyche Innovation Centre, and the national GCHQ Cyber Accelerator programme. There are also several planned investments in cyber security infrastructure over the next few years to support sectoral growth including the Cheltenham Cyber Park, and the Marches Centre for Cyber Security.

However, several consultations in the region has indicated that within the sector, investment in infrastructure has focused upon schemes supported by government and security agencies. Whilst this is welcome in growing the sector, it is viewed there are gaps in:

- **Availability and Affordability of Grade A Office Space (all sizes):** As set out by Savills[115], cyber security firms are set to take up to one million sq. ft in office space across the UK by 2022. Given the demand within the sector, combined with the need for firms to ensure working space that complies with their respective standards and accreditation (ISO 27001, Cyber Essentials etc), many consultees have identified the perceived shortage of high quality office space at all levels (for small to large teams), and the prohibitive costs associated with office rental. Increasing the supply, particularly around clusters, will support to relieve increasing office costs, and also enable concentration and collaboration between firms – thereby supporting the region's ambition to rapidly grow.

- **Provision of Product Testing and Validation Labs:** One essential process within the industry is testing products and services being offered to provide greater assurance to consumers of the overall validity of the product being offered. As such, there are several testing labs/facilities across the UK, providing CTAS and CHECK testing accreditations which identify any weaknesses utilising publicly known vulnerabilities and common configuration faults.

  NCSC has released several certified product schemes which test the validity of cyber security products and services, providing greater assurance to consumers of the reliability and effectiveness of the products they purchase, including Commercial Product Assurance, Commercial Evaluation Facilities, Commodity Information Assurance Services, Tailored Evaluation, and TEMPEST and EMS. (see Appendix H) However, some consultees argue that there is a gap that exists for an independent body to provide testing and validation labs in the region. This would enable private firms to test their

[115] Savills, *Cybersecurity firms set to take 1m sq ft of UK office space as rise in tech leads to greater threat.* Available at: http://www.savills.co.uk/_news/article/72418/228713-0/3/2018/cybersecurity-firms-set-to-take-1m-sq-ft-of-uk-office-space-as-rise-in-tech-leads-to-greater-threat

products in a space that would not necessitate a standard approach i.e. sharing all relevant code or IP with a national body.

- **Encouraging Private Investment:** As noted in Section 5.8, there are notable gaps in encouraging private investment within the region. Whilst consultees felt that funding and credit supply is relatively healthy in the sector, more could be done to encourage public-private partnerships and joint investment in projects to support business growth, skills and infrastructure.

  Within the region, firms such as QinetiQ, BAE Systems Applied Intelligence, Lockheed Martin, and Yamazaki Mazak have all provided private funding and support for cyber security and new generation investments in recent years. Indeed, the Community Cyber Security Operations Centre in Worcester also signals that firms of all sizes across the sector will support with financial and in-kind support to encourage a sustainable and diverse sector. However, where anchor firms in the region can invest in cyber security and support initiatives or work with firms in the local cyber security supply chain, this will provide commercial opportunities to grow the sector.

  There is therefore a gap to be continually reviewed regarding business commitment to investment in cyber security (at all levels) across the region, and assessment of the potential implications for supply chains.

  This is particularly important given the strong levels of Business Expenditure on Research and Development (BERD) in the region's manufacturing, automotive and defence sectors, as many of these large firms may have considerable untapped potential to invest in schemes that support the maturity of emerging cyber security capabilities e.g. securing autonomous vehicles.

- **Regional Awareness:**
  There is a consensus among consultees that the Cyber Resilience Alliance region has significant expertise, driven by the region's established national defence and security clusters

  "There is a strength in the proximity to support infrastructures, clients, and talent, particularly fed through GCHQ."

  "There is a strong bedrock of cyber experience, albeit from a military / defence standpoint, as well as a relatively strong and vibrant start-up and creative culture."

  However, there is also a perceived gap that internationally – investment in UK cyber security is often conflated with London, and that the region will need to invest in a coherent vision, brand and message to promote the area as a highly attractive location for living and working.

5.3 Opportunities

The cyber security sector clearly presents several opportunities in the region, not just for economic growth at the sectoral level, but also through securing the crucial technological developments across wider society. Ultimately, cyber security is about embedding trust in society, economy and technology, and the Cyber Resilience Alliance region will provide the expertise to support wider transformational advancement in the UK.

There are clearly opportunities that arise from automation, AI and Machine Learning, and within securing the rapid roll-out of IoT devices across the country.

5.3.1 Opportunities for R&D, Product Development and Enhancing Productivity:

The region has demonstrated in recent years that there has been a concerted effort on behalf of manufacturing in particular to increase investment in research and development. Given the opportunities that arise from automation, Artificial Intelligence, and machine learning for firms across the region, there are also core opportunities for the region's cyber security region to benefit from commercial partnerships to secure these technologies.

This increased investment in transformative digital technology in the region, combined with world-leading secure solutions, will generate considerable opportunity to enhance productivity and living standards in the region.

5.3.2 Opportunities for Resilience:

The most recent DCMS Cyber Breaches Survey (2017) indicates that 34% of businesses have no spend on cyber security, and that four in ten experienced some form of breach last year.

We will survey a wide range of firms (across sectors) to identify regional vulnerabilities and barriers to supporting a cyber resilient culture e.g. technical knowledge, finance and cost of systems, time constraints etc.

We will subsequently seek to further develop initiatives to tackle gaps in cyber resilience in the region e.g. funding for advice, Cyber Security vouchers, Cyber Club etc.

There is clear opportunity for the region to act as a regional testbed for initiatives that support cyber resilience to be scaled up to national level (evidence informed pilots and interventions).

5.3.3 Domestic and Export Growth Opportunities for the Cyber Resilience Alliance:

As identified in the UK Cyber Exports Strategy (DIT, 2018) – our region has an established, expert and innovative sector made up of companies across a full range of capabilities.

UK cyber security exports are set to grow to £2.6bn by 2021, and will be primarily driven by governments, financial services, automotive, energy and Critical National Infrastructure, healthcare and infrastructure.

The following table sets out how we will utilise our strengths to best take advantage of commercial opportunities in cyber security:

Theme	Market (2016 international spending) – Source: DIT Export Strategy (2018)	Opportunity
Government	£27.6bn	We have many established firms known internationally which work with global governments in advisory cyber security work and solutions e.g. BAE Systems Applied Intelligence has worked extensively in Asia developing SOC solutions.
Financial Services	£16.1bn	The Cyber Resilience Alliance is home to the world's largest building society (Nationwide) and an emerging cluster on FinTech / financial verification firms.
Automotive	£0.9bn	The Cyber Resilience Alliance has several firms closely tied to the UK's automotive supply chains in the North. We will work closely with Connected Midlands for identification of opportunities in securing autonomous vehicles.
Energy and Critical National Infrastructure	£0.77bn	Many energy and CNI systems are considered 'legacy' in that the technology utilised predates the security solutions considerably. We will work closely with NCSC to identify solutions, potential business partners to address and undertake security patches, and embed principles of secure-by-design.
Healthcare	£4.06bn	As evidenced by the WannaCry ransomware attacks in 2017, education, upskilling, awareness and investment are required in our health systems to ensure continuous uninterrupted running of the NHS critical services.
Infrastructure	£0.65bn	Many firms in the region work closely with infrastructure partners to ensure adequate cyber security provision e.g. Virgin Trains and IRM. We will support these relationships, in addition to investing in infrastructure that enables wider sectoral growth.

We are an outward looking region and have been recognised in the UK Cyber Exports Strategy for our commitment to growing the UK's strong cyber export base. We will therefore explore opportunities for cyber security growth through international recognition, working closely with the Department for International Trade, Innovate UK, and the Midlands Engine to promote a cohesive message about investing in the region and purchasing its products and services.

5.4 Key Ambitions and Proposals for Growth

To best tackle the gaps within the region's cyber security sector, and to take advantage of the opportunities provided by technological transformation, this section sets out our key proposals and suggested interventions for the region.

Across the four Local Enterprise Partnerships, we estimate a financial commitment to the sector over the next five years in the region of £80m (£16m per annum)[116]

Proposal 1: Innovation, Research & Development | Investing in Infrastructure

Business Expenditure on Research and Development (BERD) within the region has been increasing in recent years, and this is arguably being driven by several large manufacturing and automotive firms within the West Midlands and South West of England. There is therefore considerable potential to utilise existing clusters and networks between these firms and innovative cyber start-ups in the region to provide commercial opportunities, and to accelerate growth.

Further, the Cyber Resilience Alliance will encourage strong utilisation of upcoming investments in cyber security infrastructure, given the expectation that such initiatives (e.g. Cheltenham Cyber Park and the Marches Centre for Cyber Security) will result in increased innovation and collaboration between newly established innovative spin-outs and start-ups.

To further enable innovation and encourage continued investment in Research and Development (R&D) in the region, the Cyber Resilience Alliance propose:

1. **Promoting Existing Infrastructure Expenditure:** The region must ensure that recent proposed investments are maintained and supported; however, these must also receive investment to join-up initiatives across the region e.g. to identify the best possible incubation space for new firms depending upon their capability, capital and ambitions. Any fragmentation of cyber security infrastructure in the region may cause a disjointed approach to seeking investment for the region**.**

2. **New Infrastructure: 'National Cyber Lab':** The Audit has confirmed the initial requirement for exploring the feasibility and potential investment in a 'new specialised data centre with a flexible cyber range and dirty lab to offer organisations the chance to engage and use these facilities in the development of cyber technology and cyber defence' which can be industry-driven.

   Given the proximity of government schemes and NCSC validation facilities, this could be scoped to become a centre of national significance e.g. a National Cyber Lab, with potential sites across the wider region – linking into wider infrastructure in the region e.g. Berkeley C11 Cyber Security Centre testing labs for University of Gloucestershire students, and the launch of UK Cloud's UKCloudX[117] service in the region (a dedicated facility which provides High Assurance cloud provision for defence and government). Membership of this centre would not only allow access to the sites but also access the subject matter experts and a

[116] See Annex A (Business Cases) for further detail and rationale.
[117] See https://ukcloudx.com/

collaborative environment where partnerships could be formed to chase the larger programmes and research funding. It would further allow access to cyber skills from the traditional industrial base. This could provide the potential for international recognition of the cluster (having industry-led testing facilities with international standards to encourage product exports). This would reflect a significant financial commitment by the region to supporting the cyber security centre.

3. **Sustained Investment in Aligned Technology:** Increased investment and adoption of innovative technologies in the region e.g. Worcestershire 5G test bed, provides regional firms with significant gains in productivity, but simultaneously requires cyber security support given the proliferation in devices and data. This provides real opportunity for sectoral growth – where the Cyber Resilience Alliance is a technological world-leader, **being a world-leader in securing these technologies is a natural extension.**

Proposal 2: Encouraging Sustainable Demand:

We will support interventions that promote the growth of the cyber security sector through domestic and export sales, and through the provision of innovative new products and technologies.

We identify the following mechanism to support this proposal:

4. **Encouraging Regional Demand**: It is the view of this Audit that the region is home to world-leading and innovative expertise. However, there remains a view by regional stakeholders that London is considered internationally as central to the UK's cyber security activity.

It is therefore crucial to provide a narrative that encourages growth at the regional level, through:

- **Highlighting the strengths, offer and capabilities of the region's cyber security expertise** through investment in suitable marketing, and schemes such as 'Meet the Buyer', Knowledge Transfer Partnerships, and sharing examples of how cyber security in the region can benefit a range of sectors e.g. agri-food, manufacturing and automotive. This could include sponsoring cyber security clusters within the region to engage with wider sectoral groups (automotive, aerospace, manufacturing, agri-food);
- Utilising the existing Local Enterprise Partnership structures to **identify opportunities to bring together cyber security firms and businesses in need of secure solutions;**
- Promoting a **marketing narrative emphasising the strengths of the region as a suitable location for cyber security investment and employment**, including space, affordable housing, high living standards, transport access and infrastructure, availability of talent, and **close proximity to bodies of national significance** in cyber security (GCHQ, MoD) and Academic Centres of Excellence in Cyber Security and active cyber security universities.

Proposal 3: Improving Skills and Talent:

For any sector to be successful, it requires a sufficient and skilled workforce. The cyber security sector has experienced considerable skills and talent shortage in recent years, and this has been reflected within remuneration levels and the extent of unfilled vacancies within the sector.

However, there is substantial demand within the sector, that can facilitate high-value employment within the region where the skills and talent are invested in sufficiently to a) increase supply of labour and b) increase the skills being requested by industry. The Cyber Resilience Alliance therefore propose to:

5. **Facilitate Workforce Planning in the Cyber Security Sector for the Region**: We propose within the Cyber Resilience Alliance to establish a working group to monitor labour supply and demand in the region to enable targeted investment and interventions. This will need to consist of regional decision-makers involved in education (across all levels), business, government and the third sector.

   Further, there is compelling evidence within the region that reskilling and lifelong learning initiatives work well in meeting labour shortages and encouraging new talent into the sector. Indeed, the region's strength in national defence and security provides cyber security as a natural career progression for many of our long-term serving personnel and provides new perspective and innovation in the sector. We will seek to encourage initiatives that encourage neurodiversity in the sector (such as the Community Cyber Operations Centre), that attract younger talent to get involved in cyber security (e.g. Cyber Schools Programme), and those schemes that seek to move people away from potential cyber-crime into security roles.

6. The Cyber Resilience Alliance is a prime location for innovative approaches in encouraging new talent into the sector, and **we will monitor and seek to support funding requirements accordingly given the potential for significant increases in regional productivity as a result of increased sectoral employment**.

7. Finally, the Cyber Resilience Alliance is home to several university accredited courses in cyber security. There are also several universities adjacent to the region that offer courses in cyber security including University of Warwick, University of Birmingham, University of Bristol, Bath Spa, and University of South Wales – demonstrating the importance of neighbouring institutions. There has been considerable growth and interest in cyber security courses in the region. **We propose that the region has potential to become home to one of the UK's first 'Centres of Excellence in Education within Cyber Security',** similar to the EPSRC accredited Academic Centres of Excellence in Cyber Security Research (or the National Security Agency (NSA) /Department of Homeland Security (DHS) Centers of Academic Excellence in Cyber Defence program[118]) - which receive international acclaim, yet focus on how to teach cyber security in an applied format of benefit to employers in the region such as Raytheon, BT, Lockheed Martin and QinetiQ and support 'life-long learning' in the region.

[118] https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

Proposal 4: Focused Marketing & Sector Targeting:

The Audit has also validated that cyber security clusters work where there is a clear awareness of the anchor-driven strengths to encourage talent and investment to flow into the particular region. Within the Cyber Resilience Alliance, there is national and international recognition that cyber security activity is strong; however, there is a risk that this can become disjointed through recognition of several smaller clusters contained within e.g. Malvern, Gloucestershire, Cheltenham, and Wiltshire etc. Indeed, the geography of the region can also often mean that the West Midlands and South West can be assumed to mean 'Birmingham' and 'Bristol' respectively; which presents a challenge to the region regarding being known on the map.

This evidences the need for the Cyber Resilience Alliance to establish a unified consortium, brand and approach to attract investment and talent.

We propose to:

8. **Sustain a Cyber Resilience Alliance representative body,** combining representation from each of the four Local Enterprise Partnerships (government, business and academia), to promote the sector. The management and governance of this body could be agreed in consultation with local, regional, and national government bodies.
9. **Establish a Cyber Resilience Alliance website / dedicated support** to demonstrate how a start-up / SME / large multinational can do business in the region (e.g. access to space, labour, grants and loans, R&D tax credits, university / research support) to ensure coherency;
10. **Establish formal Cluster Partnerships,** potentially 'twinning' the Cyber Resilience Region with comparable initiatives in the United States or other countries with prominent or emergent sectors (e.g. Israel, China, or Brazil);
11. **Marketing:** Promote the region as a high-growth location with a growing and talented labour supply, with support from LEPs to invest, start and grow – where firms will be surrounded by other world-leading innovative firms and public bodies (drawing upon the Midlands Engine Cyber momentum).
12. **Intelligent sectoral targeting:** The Cyber Resilience Alliance will identify and track firms active in sectors aligned to the four LEPs growth priorities (manufacturing, agri-food, professional services) in addition to export potential (Government, Financial Services, Energy and CNI, Healthcare, and Infrastructure), and will identify their respective approach to cyber security (spending, research, relationships with regional suppliers etc.).
13. **Enhancing Opportunities for Investment:** We will explore opportunities to bring more events, and conferences (and specialist VC investors) to the region to showcase the talent and expertise of the region.

ANNEXES

Annex A: Business Cases

The Cyber Resilience Alliance Science and Innovation Audit has identified four opportunity areas in which intervention could accelerate the commercialisation of cyber security research and development, and enhance economic growth, productivity, and organisational resilience for the region and the wider UK.

Each opportunity is presented below within a high-level outline business case; a **strategic case** explaining the background to and rationale and objectives of the proposal; an **economic case** that outlines the potential benefits to the region in monetary terms (jobs and growth) in the medium and long term; a **financial case outlining the likely costs and affordability of a meaningful investment programme**; and a **management case** outlining how the initiative might be set up and managed, including any opportunities for public-private partnerships.

However, given the pace of innovation and change within the cyber security sector, the consortium will continually review and adapt these proposed interventions as required to ensure best possible value for money.

Proposal 1: Innovation, Research & Development | Investing in Infrastructure

There is considerable potential to utilise existing and clusters networks between these firms and innovative cyber start-ups in the region to provide commercial opportunities, and to accelerate growth. The Cyber Resilience Alliance will encourage strong utilisation of upcoming investments in cyber security infrastructure, given the expectation that such initiatives (e.g. Cheltenham Cyber Park and the Marches Centre for Cyber Security) will result in increased innovation and collaboration between newly established innovative spin-outs and start-ups.

To further enable innovation and encourage continued investment in R&D in the region, the Cyber Resilience Alliance propose:

1. Project Outline	
Brief Summary of the Project	**New Infrastructure: 'National Cyber Lab':** The Audit has confirmed the initial requirement for exploring the feasibility and potential investment in a 'new specialised data centre with a flexible cyber range and dirty lab to offer organisations the chance to engage and use these facilities in the development of cyber technology and cyber defence' which can be industry-driven. Given the proximity of government schemes and NCSC validation facilities, this could be scoped to become a centre of national significance e.g. a National Cyber Lab, with potential 'satellite' sites across the wider region –

	linking into wider investments pending in the region e.g. Berkeley Green testing labs for University of Gloucestershire students. A National Cyber Lab will: • Membership of this centre would not only allow access to the sites but also access the subject matter experts and a collaborative environment where partnerships could be formed to chase the larger programmes and research funding. • It would further allow access to cyber skills from the traditional industrial base. Further, a large space dedicated to testing and innovation could offer considerable potential for inspiring a new generation in cyber talent through hosting events for schools, universities, industry, and conversion course initiatives. • This could provide the potential for international recognition of the cluster (having industry-led testing facilities with international standards to encourage product exports). • This would reflect a significant financial commitment by the region to supporting the cyber security centre.
Key Partners	Partners (subject to delivery) expected to be included: • **Businesses**: It is expected that several of the large firms engaged with cyber security in the region (e.g. Raytheon) could be involved in an advisory and domain expertise capacity (e.g. CSIT Labs); however, the main beneficiaries of the Cyber Lab would be anticipated to be a range of small and medium innovative cyber security firms seeking to develop, test, adapt and validate their products in the region. • **Universities/Research Institutes**: Regional Universities could be involved to provide research, advisory and testing capacity. This includes those within the SIA region and across the UK, with potential for partnership with international universities (e.g. University of Maryland). Regional research institutes and initiatives will also be consulted for potential involvement to provide opportunity to utilise the site and resources e.g. Corsham Institute. • **Clusters & Networks**: To maximise participation and usage, the region's cyber security clusters (e.g. Malvern CSC and Cynam) will be involved. Further, the Cyber Lab would provide opportunities for firms to move from smaller incubation sites (complementary to the Cyber Park) • **Local Enterprise Partnerships** • **Innovation and Commercialisation Bodies:** We would seek to include national and regional bodies and initiatives active within innovation and commercialisation – to ensure complementarity between the NCL and other schemes (e.g. ICURE, Innovate UK, UKRI, Wayra).

	• **Validation & Accreditation Bodies**: It is anticipated that a National Cyber Lab would require steering by an agreed validation body (following for example, the Cyber Essentials Scheme).
2. Strategic Case	
Rationale for Intervention	The proposed development of a National Cyber Lab within the region is focused upon: • Providing Product Development and Testing Facilities: These would be within a secure setting and would explore opportunities for firms seeking to commercialise and develop products to do so without restriction / loss of intellectual property. • Training and Simulation Facilities: A NCL could provide space for training and simulation for a wide range of stakeholders (at limited cost) to schools, businesses, universities etc. • Demonstration: A NCL could provide opportunities for product demonstration, and host international trade events (as set out in proposal 4). • Would support to incubate start-ups and grow small and medium firms – thereby supporting the region's status as the UK's leading cluster of cyber security activity (outside London), and showcasing the benefits of the region for high-skill and competitive cost of office space/ cost of doing business. • Embedding a 'central lab' for UK activity, whilst ensuring a series of networks (smaller sites across the region and wider UK, enabling access to office space, incubation, nodes)
Links to Existing Policy & Existing Gaps in Provision	A National Cyber Lab would strategically complement the UK Government's Industrial Strategy, and the UK National Cyber Security Strategy. **Industrial Strategy:** "*If the UK is to be the most innovative country in the world, we need to be able to capture the value from our science, research and creativity and support innovations that drive our productivity."* **UK National Cyber Security Strategy** The National Cyber Security Strategy (2016-21) is a pivotal strategy for the Cyber Resilience Alliance. It sets out proposed investment of £1.9bn in supporting the cyber security sector, and its innovation, research and development over the five years. It recognises that whilst the initial National Cyber Security Strategy (2011) was beneficial in helping the UK become a leading global player in cyber security, there is more to achieve in the years ahead, including:

	• Too many networks, including in critical sectors, are still insecure. • The market is not valuing, and therefore not managing, cyber risk correctly. • Too many organisations are still suffering breaches at even the most basic level. • Too few investors are willing to risk supporting entrepreneurs in the sector. • Too few graduates and others with the right skills are emerging from the education and training system."[119] A National Cyber Lab would support businesses to validate, promote and sell innovative solutions to market to help tackle these gaps in UK cyber security, and to support and grow the sector.
Potential Scope of the Project	Whilst based in the Cyber Resilience Alliance region (potentially with a 'main site' in an easy-to-access urban location – to be decided, with satellite access across the region), the project will seek to be nationally focused.
3. Economic Case	
Anticipated Benefits and Risks	A National Cyber Lab would cement the position of the region as a leading cluster of cyber security innovation globally. It would also complement existing assets and pending investments in the region, including linking into the Cheltenham Cyber Park, C11 at Berkeley Green, Malvern Hills Science Park, and the Marches Centre for Cyber Security. Anticipated benefits include: • A private and secure space for small and medium enterprises to test and validate innovative and world-leading cyber security projects to translate into commercial outcomes; • Clearer opportunities for the region's strong security and defence, and manufacturing and automotive sectors to utilise 'developed in region' cyber security products and processes within their own supply chains; • Enhanced collaboration between business, universities and education, and Government to grow the sector and meet the objectives of the NCSS and Industrial Strategy; • Provision of further national infrastructure, adjacent to the UK's core defence assets (GCHQ and MoD). This will improve the scale and talent within the region in cyber security – providing a significant cluster of talent for national security to draw upon to support securing the nation's digital assets.

[119] HM Government, *National Cyber Security Strategy 2016-2021*, pg 27. 2016. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

	Potential Risks include: • The creation of a new National Cyber Lab, if not managed clearly, could cause potential for confusion with other assets (e.g. SMEs unclear whether to utilise these facilities or other assets across the region). This will be mitigated through a clear vision and purpose for the centre, including eligibility criteria and signposting through the Cyber Resilience Alliance structures.
Likely Costs	The proposal for a National Cyber Lab has not been subject to a full business case or feasibility study (the Cyber Resilience Alliance will explore opportunity to do so, to ensure that any proposed infrastructure best reflects likely usage, and value for money). However, it is anticipated that a National Cyber Lab should be developed at a significant scale given the preference for national reach (enabling businesses, universities and government nationally to participate). Initial discussion of the project within the Cyber Resilience Alliance has indicated that a NCL could cost approximately £15-25m in capital costs, with subsequent running costs associated with a modest team, which could be supported by the LEPs and universities (revenue and or in-kind) with potential for an external body to be procured to deliver the running of the Lab.
4. Commercial Case	
Can the project be delivered? Is it viable?	Yes, subject to business case and partner support.
5. Financial Case	
Is the required funding available?	Not at this stage. The LEPs involved within the Cyber Resilience Alliance have demonstrated commitment to utilise Growth Deal funding to promote the cyber security sector (see Cheltenham Cyber Park and Marches Centre for Cyber Security for example). Funding from Government could be, where appropriate and available, be matched accordingly.
6. Management Case	
How will the project be managed? Is there significant capacity?	To be confirmed subject to further business case. However, a project of this scale would require significant formal collaboration and co-ordination, with clear project management procedures. Further work will be required to explore the most effective project management approach going forward.

Other Actions within this Opportunity (not subject to business case):

a) Promoting Existing Infrastructure Expenditure: The region must ensure that recent proposed investments are maintained and supported; however, these must also receive investment to a) join-up initiatives across the region e.g. to identify the best possible incubation space for new firms depending upon their capability, capital and ambitions. Any fragmentation of cyber security infrastructure in the region may cause a disjointed approach to seeking investment for the region.

b) Sustained Investment in Aligned Technology: Increased investment and adoption of innovative technologies in the region e.g. Worcestershire 5G test bed, provides regional firms with significant gains in productivity, but simultaneously requires cyber security support given the proliferation in devices and data. This provides real opportunity for sectoral growth – where the Cyber Resilience Alliance is a technological world-leader, being a world-leader in securing these technologies is a natural extension.

The table below reiterates the pending investment over the next four years within cyber security projects within the Cyber Resilience Alliance.

Project	Pending Investment:
Cheltenham Cyber Park:	£22m
Marches Centre for Cyber Security	£9m
Malvern Hills Science Park	£4m
NMITE	£9m
C11 at Berkeley Green	£3m

Proposal 2: Encouraging Sustainable Demand:

We will support interventions that promote the growth of the cyber security sector through domestic and export sales, and through the provision of innovative new products and technologies.

1. Project Outline	
Brief Summary of the Project	**'**Encouraging Demand' consists the provision of a narrative that encourages growth at the regional level, through: • **Highlighting the strengths, offer and capabilities of the region's cyber security expertise through investment in suitable marketing**, and schemes such as 'Meet the Buyer', Knowledge Transfer Partnerships, and sharing examples of how cyber security in the region can benefit a range of sectors e.g. agri-food, manufacturing and automotive. This could include **sponsoring cyber security clusters within the region to engage with wider sectoral groups** (automotive, aerospace, manufacturing, agri-food); • Utilising the **existing Local Enterprise Partnership structures** to identify opportunities to bring together cyber security firms and businesses in need of secure solutions; • Promoting a **marketing narrative emphasising the strengths of the region as a suitable location for cyber security investment and employment**, including space, affordable housing, high living standards, transport access and infrastructure, availability of talent, and close proximity to bodies of national significance in cyber security (GCHQ, MoD) and Academic Centres of Excellence in Cyber Security and active cyber security universities.
Key Partners	It is intended that partners within these interventions will grow over time, and include: • Businesses (including large firms influential in the region's supply chain e.g. QinetiQ, Dyson, Lockheed Martin etc.; small and medium size innovative cyber security firms) • Businesses not currently engaged or aware regarding cyber security initiatives to be joined-up to resilience initiatives e.g. The Cyber Club, attending LEP cyber security events • Universities • Further Education • Schools • Local Enterprise Partnerships • Local Authorities • Local Health Authorities / Clinical Commissioning Groups

	• TechNation • Industry Associations / Representative Bodies
2. Strategic Case	
Rationale for Intervention	A clear promotional and marketing initiative to secure the region's position as being known globally as a hotbed for cyber security innovation will support wider initiatives in the region and help to enhance the international reputation and investment for the Cyber Resilience Alliance region.
Links to Existing Policy & Existing Gaps in Provision	In addition to the National Cyber Security Strategy (Developing the sector), and the Industrial Strategy, promotional activity should also support DIT's Cyber Exports Strategy, helping to grow the UK's cyber security from £1.5bn (2017) upwards.
Potential Scope of the Project	This will be focused on the Cyber Resilience Region area and will seek to complement (and avoid duplication with) the wider 'Cyber Valley / Midlands Engine Cyber initiatives.
3. Economic Case	
Anticipated Benefits and Risks	The benefit of this intervention will be attained through ensuring that cyber security investments across the region are well-known, utilised, and developed to meet the needs of industry – which will ultimately support wider sustainable economic growth.
Likely Costs	It is expected that the costs of this proposal can be met largely through the existing Local Enterprise Partnership, and central government budgets. The costs could be variable subject to funding and coherency of brand (in the region of £100k – 500k per annum subject to number of events and initiatives).
4. Commercial Case	
Can the project be delivered? Is it viable?	Yes, there is experience of similar initiatives being undertaken within the LEP structures, and the Cyber Resilience Alliance is committed to a joint approach in branding and funding to ensure a coherent message regarding the cyber security sector in the region.
5. Financial Case	
Is the required funding available?	Yes – the Local Enterprise Partnerships will explore the potential for funding subject to cost. However, they will identify where efficiency can be maximised through collaboration with other bodies e.g. DIT Cyber Exports, or the Midlands Engine Cyber initiative.
6. Management Case	

How will the project be managed? Is there significant capacity?	Delivery will be managed through the Local Enterprise Partnership structures, potentially with one LEP as a lead role, and the remaining LEPs and stakeholders participating in a project steering group with appropriate governance structures in place.

Proposal 3: Improving Skills and Talent:

For any sector to be successful, it requires a sufficient and skilled workforce. The cyber security sector has experienced considerable skills and talent shortage in recent years, and this has been reflected within remuneration levels and the extent of unfilled vacancies within the sector.

However, there is substantial demand within the sector, that can facilitate high-value employment within the region where the skills and talent are invested in sufficiently to a) increase supply of labour and b) increase the skills being requested by industry.

The Cyber Resilience Alliance therefore propose to:

1. Project Outline	
Brief Summary of the Project	The key actions associated with this proposal include: • Facilitation of Workforce Planning in the Cyber Security Sector for the Region: We propose within the Cyber Resilience Alliance to establish a working group to monitor labour supply and demand in the region to enable targeted investment and interventions. This will need to consist of regional decision-makers involved in education (across all levels), business, government and the third sector. • We will seek to encourage initiatives that encourage neurodiversity in the sector (such as the Community Cyber Operations Centre), that attract younger talent to get involved in cyber security (e.g. Cyber Schools Programme), and those schemes that seek to move people away from potential cyber-crime into security roles. • The Cyber Resilience Alliance is a prime location for innovative approaches in encouraging new talent into the sector, and we will monitor and seek to support funding requirements accordingly given the potential for significant increases in regional productivity as a result of increased sector employment. • We propose that the region has potential to become home to one of the UK's first 'Centres of Excellence in Education within Cyber Security', similar to the EPSRC accredited Academic Centres of Excellence in Cyber Security Research which receive international acclaim yet focusing on how to teach cyber security in an applied format of benefit to employers in the region such as Raytheon.

Key Partners	As per Proposal 2
2. Strategic Case	
Rationale for Intervention	The rationale underpinning this proposal is the well-recognised shortage in labour and talent available to the cyber security sector (with demand for roles outstripping supply, which is impacting upon business capacity to grow, recruit and retain staff.) However. there is strong evidence within the region that reskilling initiatives work well in meeting labour shortage and encourage new talent into the sector. Indeed, the region's strength in national defence and security provides cyber security as a natural career progression for many of our long-term serving personnel and provides new perspective and innovation in the sector. Intervention that supports to promote awareness and encourage a career in cyber security, alongside world-class research and training will help to ensure the UK's place as a global leader in the sector.
Links to Existing Policy & Existing Gaps in Provision	The Industrial Strategy sets out a number of initiatives that are intended to help tackle the known digital and cyber security skills gap, throughout all ages and backgrounds. This includes: • £20m for the Cyber Discovery programme – a four-year study programme for the next generation of cybersecurity professionals (Cyber Schools Programme). DCMS expect the programme to reach nearly 6,000 participants by 2021. • The Government will invest £84m over the next five years to deliver a comprehensive programme to improve the teaching of computing and drive up participation in computer science, with a particular focus on girls. Measures include up-skilling 8,000 computer science teachers - enough for one in every secondary school - and working with industry to set up a new National Centre for Computing Education to produce training material and support schools The Cyber Resilience Alliance will work closely with DCMS, DfE, BEIS and the Cabinet Office where possible to provide vehicles for delivering skills and training schemes. Further, it will draw upon close relationships with schemes such as the Cyber Club, Cyber Security Challenge, SANS Institute, the Corsham Institute, and the Community Security Operations Centre in Worcester to maximise opportunities for skills development.

Potential Scope of the Project	Whilst focused within the SIA region, we recognise the need to share learning and be involved in initiatives on a national and international basis in a reciprocal way.
3. Economic Case	
Anticipated Benefits and Risks	The anticipated benefits include: • Providing opportunities within the region for high-value employment, improving GVA, productivity and exports in the region – as well as enhancing quality of life; • Upskilling our population – which will not only support the cyber security sector but all sectors (through embedding cyber resilience, enhancing awareness of coding and automation etc.) • Tackling inequalities of access to employment: as a region, we will support initiatives that improve diversity, gender equality, and neurodiversity in the sector. It is not anticipated there are any significant risks.
Likely Costs	The region will support initiatives on a case-by-case basis, exploring opportunities for alignment between the region's skills initiatives, and central government schemes (e.g. DCMS Cyber Security Skills Immediate Impact Fund)
4. Commercial Case	
Can the project be delivered? Is it viable?	Yes – there is a strong track record of partnership working in skills development.
5. Financial Case	
Is the required funding available?	Limited – whilst there is some funding available through Central Government and the LEP structures, the Cyber Resilience Alliance will seek to explore and fund initiatives that are considered feasible and will contribute to employment outcomes in the sector.
6. Management Case	
How will the project be managed? Is there significant capacity?	Initiatives will be managed on a case-by-case basis.

Proposal 4: Focused Marketing & Sector Targeting

This proposal evidences the need for the Cyber Resilience Alliance to establish a unified consortium, brand and approach to attract investment and talent. The costs associated with these recommendations are anticipated to be limited and met by the LEPs where appropriate (drawing upon other funding resources as available). The table below sets these out with potential cost and management approach per the principles of the outline business cases for the other proposals.

Approach	Potential Cost / Management
Sustain a Cyber Resilience Alliance representative body, combining representation from each of the four Local Enterprise Partnerships (government, business and academia), to promote the sector.	Limited cost – to be met by four LEPs The management and governance of this body will be agreed in consultation with local, regional, and national government bodies.
Establish a Cyber Resilience Alliance website / dedicated support to demonstrate how a start-up / SME / large multinational can do business in the region (e.g. access to space, labour, grants and loans, R&D tax credits, university / research support) to ensure coherency;	Limited cost – estimated to include start-up cost of a website, hosting, maintenance – with potential for recruitment of a representative staff member to manage the content.
Establish formal Cluster Partnerships, potentially 'twinning' the Cyber Resilience Region with comparable initiatives in the United States or other countries with prominent or emergent sectors (e.g. Israel, China, or Brazil);	Limited cost - expected to include travel / accommodation / event costs for international partnerships and events. To be managed by the Cyber Resilience Alliance, and to liaise closely with the Department for International Trade.
Marketing: Promote the region as a high-growth location with a growing and talented labour supply, with support from LEPs to invest, start and grow – where firms will be surrounded by other world-leading innovative firms and public bodies.	Limited cost – to include branding / PR as required. To be managed by the Cyber Resilience Alliance.
Intelligent sectoral targeting: The Cyber Resilience Alliance will identify and track firms active in sectors aligned to the four LEPs growth priorities (manufacturing, agri-food, professional services) in addition to export potential (Government, Financial Services, Energy and CNI, Healthcare, and	To be reflected in activities undertaken by Cyber Resilience Alliance (e.g. LEP market intelligence and sector monitoring)

Infrastructure), and will identify their respective approach to cyber security (spending, research, relationships with regional suppliers etc. via survey). We will also monitor the extent of digital innovation within the region, including business adoption of automation techniques, Artificial Intelligence, Machine Learning and IoT.	
Enhancing Opportunities for Investment: We will explore opportunities to bring more events, and conferences (and specialist VC investors) to the region to showcase the talent and expertise of the region.	To be managed by the Cyber Resilience Alliance

Annex B: How the SIA was developed

This annex sets out how the Cyber Resilience Alliance Science and Innovation Audit was developed, and summarises the background to the SIA, and the steps taken to gather the evidence base for this exercise.

Background

In Autumn 2015 the UK Government announced regional Science and Innovation Audits (SIAs) to catalyse a new approach to regional economic development. SIAs enable local consortia to focus on analysing regional strengths and identify mechanisms to realise their potential.

In Gloucestershire (GFirst), Worcestershire, The Marches (Shropshire, Herefordshire, and Telford and Wrekin), and Swindon and Wiltshire Local Enterprise Partnerships (LEPs), the **Cyber Resilience Alliance** was formed in 2017 to focus on the regional strength in cyber security.

Methodology:

In March 2018, the Cyber Resilience Alliance commissioned the development of the Science and Innovation Audit, with support from RSM (consultancy practice to lead the composition of the study) and Technopolis (the national contractor to BEIS, responsible for supporting all SIAs across the UK in this wave (Wave 3).

The Audit was overseen by a Strategic Steering Group (see Annex D) which consisted of LEP, business, and university representative, which met on a monthly basis.

Preparation of the SIA involved:

- **A Call for Evidence:** In March and April 2018, universities, LEPs, businesses and representative bodies were invited to submit evidence for utilising with the SIA; this provided a baseline regarding the number of firms active within the region in cyber security, associated skills and employment, and informed the asset identification across the region.
- **Analysis of Primary and Secondary Data:** For this SIA, Technopolis (national contractor to BEIS) provided a core data set, which included key data for the region (population, economic performance and productivity, research institutions (Gateway to Research), business counts, REF output data etc). This was supplemented with bespoke analysis undertaken by Technopolis exploring research activity in cyber security and data science within the region. RSM carried out further analysis of the size and scale of the cyber security sector within the region, and analysis of the VC sector utilising Beauhurst.
- **Literature Review and International Benchmarking:** This included a desk review of the LEP's economic priorities, UK policy (regional and national), and horizon scanning and technology forecasting for the SIA's themes.
- Fifteen **one-to-one consultations** with businesses, universities, representative bodies and government – exploring the development of firms and institutions, and views regarding the sector and region.

- An **online survey of regional stakeholders, with almost fifty full responses**: This explored stakeholder views on the size and scale of the sector, and views on the strengths, weaknesses, opportunities and threats regarding the development of the cyber security sector.

Annex C: Consultations

In April and May 2018, the consortium held an online survey for regional stakeholders (across academic, business, and public organisations) to set out their views regarding the strengths, weaknesses, opportunities and threats for the regional cyber security sector, in addition to potential investment and support they would like to see encouraged to further sustain and grow the sector.

This section sets out a **summary** of the consultation feedback received throughout this SIA exercise, including key feedback from respondents. In total, the online survey received 47 (full) responses, and a further 15 stakeholders were consulted for in-depth one-to-one consultations regarding the sector.

Strengths and Weaknesses in the Region

Q) What are the major strengths of the cyber security sector in the Cyber Resilience Alliance region?

"Proximity to support infrastructures, clients, talent, particularly fed through GCHQ."

One medium sized information management specialist highlights the proximity to large government departments as an influential factor in the success of the region, in addition to the close proximity to major cities, such as Birmingham and Bristol, which makes acquisition of new clients much easier.

The managing director for an Information Assurance SME recognised that GCHQ proximity has meant there is *"an abundance of technically astute/intelligence/security focussed people who have settled in the area"* which has brought credibility to the region. Talent is also thought to be developed by the Ministry of Defence's Cyber School located alongside Cranfield University. The school has launched a Cyber master's level teaching course to upskill local talent and ensure the skills demand gap in the area is sufficiently met.

"There is a strong bedrock of cyber experience, albeit from a military / defence standpoint, as well as a relatively strong and vibrant start-up and creative culture, originating in Bristol." Voluntary Sector Cyber Security Organisation Representative.

Several respondents find the strength of the local cyber security ecosystem the region's biggest strength, benefiting from a combination of traditional cyber services provided by established companies, flourished with a selection of niche companies which are developing cutting edge technologies which drive progress in the sector and act to support innovative activities in the sector across the region.

"There is a mix of capability - some of which is world-class - across government, academia and industry." CTO for a Large Defence Technology Company.

One poignant observation emerged as respondents noticed a changing trend in defence and security organisations building and implementing cyber solutions, in particular, for Critical National Infrastructure (CNI) security. Often these large firms work in tandem with niche technology developers, as well as academic researchers to create tailored products, demonstrating the importance of industry-academic links, but ultimately, a strong local ecosystem with a vivacious start-up culture.

Q) What are the major limitations for the cyber security sector in the Cyber Resilience Alliance region?

"Sub optimal demand for Cyber Security services when compared to London/South East." Information Risk Management SME Founder.

The focus to grow the London/South East cyber security cluster is diverting activity away from the Cyber Resilience Alliance region. Several respondents highlighted this as an issue, with one noting the annual GCHQ sponsored Information Assurance exhibition and associated presentations are usually hosted in London. They argued events like this should be moved to Cheltenham, bringing with it expertise to the region, rather than satiating the London market and neglecting other growing clusters across the UK.

"Struggle to attract people with the correct experience and skillsets in Cyber Security." SME IT infrastructure security and digital marketplace employee.

A significant portion of small and medium sized companies brought to light the skills demand gap in the region for talented labour. As is a common theme, London appears to attract the best talent, leaving other parts of the UK with less option for recruitment. Respondents noted that the Cyber Resilience Alliance region is not the only cyber security cluster fighting for cyber security specialists, commenting on Manchester and the North's growing presence in the sector. The founder of an Information Risk Management SME commented that *"Talent is the largest single limiting factor to the growth of UK cyber Security companies and the market. Low talent concentration leads to inflated salary costs, and a barrier of entry for new innovative start-ups."*

"There is a lack of accelerator/incubator foundations." Voluntary Sector Cyber Security Organisation Representative.

Some respondents have found the current support system in the UK to be quite "toxic" and needs revamping in order to adequately support start-ups. Rather than supporting a lot of companies with relatively little individual support, there should be a change of support culture in which there is a genuine desire to see these companies grow. One respondent went so far as to say that the ecosystem for start-ups and innovation simply isn't present in the area. The respondent suggested greater publicity of successes in the sector from key players in the Cyber Resilience Alliance region could rectify the issue.

"Infrastructure is poor, both in terms of physical and digital." CTO for a Large Defence Technology Company.

Q) Which product, service or sub-sector of cyber security do you believe the Cyber Resilience Alliance region should be backing (or focused upon supporting) in the next five years?

"Autonomous systems are a juicy target for cyber criminals and we need to assure ourselves that they are safe to use from a cyber perspective otherwise the market will fail." Business Director for a Software Systems Security SME.

There was a mixture in opinion from respondents as to the focus or direction which the Cyber Resilience Alliance should steer towards, although a common theme was developing automotive data and assurance of autonomous systems, as well as other advanced manufacturing system assurance. The underlying feature which instructs autonomous vehicle technology is the Internet of Things; this was another common theme of application which respondents would like the Cyber Resilience Alliance to focus on.

Others highlighted artificial intelligence and vulnerability monitoring and resolution as areas of high-growth potential which have the added benefit of bringing other solutions across the sector to the market quicker.

"There should be training providers outside of academia to support the development of new talent and to teach the skills and industry qualifications required and often mandated." Information Risk Management SME founder.

Many of the respondents were of the opinion that product and service focus were considered secondary areas of attention for the sector. Rather they should get the skills and training right in the area. It was even suggested that Local Authorities and Central Government should upgrade their systems and other cyber security related services with local cyber security companies support, helping to grow the local ecosystem.

Other areas of product and service focus included, although to a lesser extent, governance, risk management, effective and pragmatic policies, process, procedures; cloud security; penetration testing; and, threat assessments.

Local Support Systems

Q) Are there any policies or supports your organization would like to see enacted to promote and enhance the sector in the region?

"We should establish 'cluster partnerships' so the region could be 'twinned with Silicon Valley'." Cyber Security Investment Company Founder.

Respondents would like to see stronger engagement with international players and funding streams. One respondent would like to see a change in work visas to encourage active research partnerships with the international community such as the US, Israel and Asia. This should act to facilitate the movement of talent and consequently, knowledge transfer. Building on this, the respondent noted that the Cyber Resilience Alliance region could twin itself with foreign clusters.

An example of this recently has been in 2016, whereby the Midlands Engine Cyber mission took cyber security companies of all sizes from across the Midlands area to Baltimore, Maryland to attend the CyberMaryland Conference. In return, during June 2017, companies from Maryland and the Midlands participated in a five-day Info Security Europe Conference in the Midlands, providing opportunity to share information and business opportunities. Drawing in more than 10,000 visitors, the event showcased local cyber security capability and the potential investment opportunities within the Midlands cyber sector.

Other respondents would like to see full and guaranteed access to Horizon 2020 funding. Currently UK government funding is small by comparison and only draws on UK expertise. It is hoped that international streams from within the EU and USA will offer support beyond what is currently available to young start-ups.

"Sponsor the West of England Cyber Cluster in order to allow its meetings to take place on a regular basis." Voluntary Sector Cyber Security Organisation Representative.

Respondents were keen to see stronger engagement between the Cyber Resilience Alliance and the region. Sponsorship of the West of England event would ensure the cyber community remain fully informed on key developments in the sector, as well as to identify the collective viewpoint of the sector in the region. One respondent highlighted the existing stellar links to BusinessWest and to the Department of International Trade, and that relations with the Cyber Resilience Alliance would not go amiss.

"Standards have to be developed and policed for autonomous systems." Business Director for a Software Systems Security SME.

Expanding on the overwhelming consensus that autonomous vehicle systems are an essential part of the Cyber Resilience Alliance region's capability, one medium sized company believed that as the autonomous systems market develops there has to be regulatory involvement to ensure that these systems are secure in order to support the safety case.

"Support for staff training, whether at a dedicated centre near NCSC or at a network of colleges throughout the region." Business Development Manager for a Cyber Security SME.

For smaller companies in our sample, there was a common theme of greater support in identifying talent for young start-ups, as well as other learning opportunities which could be further developed in the region.

Higher and Further Education Engagement in the Region

Q) Which universities and / or Further Education institutions do you engage with for the purposes of encouraging cyber security R&D?

One public sector organisation representative highlighted their work with the University of Wolverhampton and the upcoming cyber technology centre under development in Herefordshire. The University of Wolverhampton was also praised for its existing provision through its campuses in Wolverhampton and Telford.

Some respondents currently engage with Academic Centres of Excellence in Cyber Security Research, including Imperial College London and Royal Holloway, University of London, Bristol University, Centre for Secure Information Technologies (CSIT) at Queen's University, Belfast and Warwick University.

With regard to local universities within or near the region, some respondents found that the University of Bristol had particular R&D strengths in cryptography, while others commended additional work in the Bristol area; Bath Spa University are considered to be on the leading edge in terms of digital creativity, and will soon contribute to the cyber talent pool in the local area as they develop their upcoming Cyber BSc and MSc.

Despite the concerted effort in the region to develop the autonomous and advanced manufacturing industry, only one respondent highlighted the autonomous systems capability among local universities and further education institutions. This may be indicative of an ecosystem with start-ups developing their own autonomous systems security, rather than larger companies engaging with academic institutions to develop novel technologies in the sector.

To gain insight on how the industry should move forward, respondents were asked what cyber security R&D challenges they would like to see academic institutions tackle. Building on previous discussion, although not applicable to R&D, firms would like to see enhanced provision of skills among young talent. However, the most common area for future development was highlighted as quantum computing and cryptography, while others would like to see greater emphasis on IoT research.

Cyber Security Labour Force in the Cyber Resilience Alliance Region

Q) What do you think of the local labour market for cyber security sector in the Cyber Resilience Alliance region?

There was no majority opinion regarding the regional cyber security labour market; roughly half of the sample respondents believed the current market to be fairly sustainable, while the other half believed it to be fairly unsustainable.

"Recruitment is always a challenge in an area with a relatively sparse population and no major city, but once staff are recruited, they tend to be easy to retain." Business Development Manager for a Cyber Security SME.

To maintain a fairly sustainable labour force, some respondents noted they target universities nationally as they're well-positioned to provide the formal methods skills needed by industry. One small firm has onboarded two apprentices, demonstrating capacity to develop skills in-house.

One point made was that the life of a cyber operative currently is to be on the road, visiting clients regularly. As such, the respondent thinks this lifestyle can be sustained if there are

additional attractions, outside of money, which will attract talent to the Cyber Resilience Alliance region. The proximity of Bristol, a major UK city, was discussed as a potential attraction.

"As this is an emerging market and the build-up of cyber requirements is expediential, developing and retaining a resource pool to support this is going to be a challenge." SME IT infrastructure security and digital marketplace employee.

Respondents were aware that despite the vast sums of money disseminated to deal with the skills shortfall - the major focus of which has been expanding university places - there still exists an issue of matching the skills of graduates with industry. One respondent noted the majority of graduates are still not sufficiently skilled to take a job in industry, and consequently are burdened with having to train graduates and put them through industry qualifications. The impression is that this starves the smaller enterprising companies who cannot afford to subsidise these industry qualifications, meaning the SME becomes a feeder for the T1 suppliers which in turn fuels salary inflation.

Beyond this, the disarray in industry qualifications, alongside complexities in the industry has meant that new talent wishing to transition from e.g. an IT support role to a cyber security role are facing barriers to entry.

"The lights of London will continue to shine brightest and attract the talent." Cyber Security Investment Company Founder.

One sentiment among respondents was that London is the draining key talent from the Cyber Resilience Alliance region. Some believed that until the CRA region is a recognised cyber hub, talent will move elsewhere around the country. Due to differences in access to finance, particularly for the SME community, start-ups are more attracted to London; this was highlighted as a key factor to address in overcoming shortfalls in the regional cyber force. One respondent was keen to elucidate on the efforts of organisations such as GCHQ and QinetiQ in attracting talent to the area, although remained concerned about the pull of the London / South East bias.

"Bring together the various initiatives and ideas into a central group so that they understand each other's roles and how to support." Voluntary Sector Cyber Security Organisation Representative.

Respondents were asked about what actions could be taken to build the pool of local cyber security talent. Most respondents were of the impression that engagement between education institutions and industry would be the best solution to ensure the correct skills are being developed. One example given was to encourage the local area to partner with a UK charter, such as the IET, to help shape the industry from careers, to standards, to educating the market.

Others believed that more responsibility should be placed on schools to communicate cyber security awareness, highlighting the potential path which comes with a career in cyber security. As part of this, respondents of all company sizes were convinced that apprenticeships are an effective channel to engage with young talent at an early stage, building their skills alongside industry requirements.

Local Physical Infrastructure for the Cyber Security Industry

Q) What is the local physical infrastructure for the cyber security industry like in the region, and how could it be improved?

Our sample of respondents were split in opinion in terms of the quality of local physical infrastructure. One third believe it's fairly or very strong, another third believes it either very or fairly weak, while one third believe it's neither weak nor strong.

"The new Worcester Parkway station is a game-changer, opening up Cheltenham and Bristol." Software Security SME Founder.

Those with positive sentiment gave adequate road and rail links, particularly the M4 between Swindon and Bath, and a large talent pool on the doorstep as reasons why this is the case. The push for innovation activities in the Bristol / Bath area has meant physical infrastructure in and around the Cyber Resilience Alliance region has improved.

Despite this positive sentiment, these respondents still suggested practical actions to help build the physical infrastructure. The majority thought connectivity could be improved, suggesting enhanced fibre rollout, greater connectivity for rural players, and enhanced communications infrastructure for nomadic workers. One respondents suggested *"the introduction of a local Government approved data-centre that can store classified material for the significant base of local customers in the region."*

"It is difficult to get across the region and links out of the region are not high speed and from some parts very expensive." Large Defence Technology Company CTO.

Conversely, those which were unimpressed with the local physical infrastructure felt neglected, highlighting issues with transport links as the main reason for their dismay with local infrastructure. One respondent located in Welshpool was shocked that despite being on both the main North-South and East-West routes in Wales, the nearest dual carriageway is 20 miles away. Others suggested improvements could be made to local public transport as it is currently deemed non-existent.

To rectify these issues, respondents thought that simple improvements in local transport links, such as rail and road, should take priority. Others had specific action plans to ensure the most effective use of public money to improve infrastructure; a long-term view should be taken to identify the key hubs of activity in the region, and the corresponding commuter routes to these hubs, and develop a new transport system making use of this information.

Annex D: Cyber Resilience Alliance Consortium

Steering Group Membership:

Gary Woodman: Worcestershire LEP

Gary is tasked with driving forward Worcestershire LEP and leading an Executive Team to support the WLEP's ambitions and delivery of the WLEP business plan. From his former role as Head of Policy and Education at Herefordshire and Worcestershire Chamber of Commerce, he has brought with him a wealth of business insight and networks as well as considerable experience of Government policy and delivery. Educated at the University of Wales, Cardiff, where he obtained his degree in Leisure and Recreation Management, and the University of Gloucestershire, where he studied for his postgraduate diploma in Business Administration, he previously worked for Gloucestershire County Council's market towns and economic development arm, overseeing regeneration.

Nicola Whiting: Titania

Nicola Whiting is an experienced Chief Operations & Strategy Officer with a strong history of working in Cyber Security / InfoSec. Specialising in enterprise security automation software (self-healing networks), business development, trust-based selling and neuromarketing.

An advocate for Autism and Women in Cyber, she provides government level advice on Diversity and writes for publications such as *The Huffington Post, Defence Contracts Bulletin, Defence News Online and Signal.* A well regarded public-speaker keynote topics include "The Rise of Automated Attacks", "The Future of Automated Cyber Defences" and "Hacking the Human Brain".

In 2017 Nicola was named by SC Magazine as one of the Top 20 most influential women working in cyber security.

Professor Ian Oakes: University of Wolverhampton

Over the last 20 years, Professor Oakes has held a number of senior management posts in higher education before joining the University of Wolverhampton in 2008 as Pro Vice-Chancellor with responsibility for the University's research and enterprise agenda and developing the growing knowledge transfer arena at regional, national and international levels. More recently he was promoted to the role of Deputy Vice-Chancellor as well as Chief Executive of University of Wolverhampton Science Park.

Professor Kamal Bechkoum, Professor of Computing, is Head of The School of Business & Technology at The University of Gloucestershire. He is a Gloucestershire Commissioner for Cyber, Science and Innovation and the University lead of a £3m Cyber Security project, working with other organisations to produce highly skilled cyber professionals in Gloucestershire and beyond. Professor Bechkoum has also worked at Cranfield, De Montfort, Wolverhampton, Derby, and Northampton where he was Executive Dean of the School of Science and Technology with university executive responsibility for research and enterprise and intellectual capital. He holds a PhD in Software Techniques for Computer Aided Engineering from the University of Cranfield, UK and is a Fellow of the British Computer Society and a Chartered IT Professional.

Professor Richard Benham is the world's first formal Professor of Cyber Security Management and lectures at Coventry Business School and at the UK's National Cyber Skills Centre where he is Professor in Residence. He is also a Visiting Professor in in Cyber Security Management at The University of Gloucestershire and previously in Policing at Staffordshire University. Outside of the UK, Prof Benham is a SWIFT Institute Scholar and speaks at one of the World's leading Business schools, IMD in Switzerland. In 2013 he published "The Cyber Ripple Theory®" which is widely recognised as the World's first Cyber Management Theory and includes the human elements of Cyber Security. In 2017 he was chosen to join the DL100 and was nominated for UK Digital Champion of the Year. He is currently the Digital Champion for the South West.

Mark Pearce: Skylon Park: Mark is the Managing Director of Hereford Enterprise Zone Limited, a private/public partnership company charged with catalysing business investment at Skylon Park, the only Enterprise Zone in the country with a defence and security focus. In his 6 years at Skylon Park, over 37 acres of land has been sold, 41,000 sq m of new workspace built or committed, 38 businesses moved in and over £20m of private sector investment secured, with more sales and projects in the pipeline. An economic development professional of nearly 30 years standing, Mark worked previously at the West Midlands Regional Development Agency, Advantage West Midlands (AWM) for over 10 years, latterly as Corporate Director. He oversaw significant investment into urban and rural regeneration in the West Midlands including longstanding Board representation at Hereford Futures, the £100m+ mixed use project that has transformed Hereford City Centre. He moved to AWM after

extensive experience in rural regeneration policy and delivery at a national, regional and local level.

Kathryn Jones: Marches LEP: Kathryn joined the Marches LEP team in October 2017 as Partnership Manager. She has a background in economic development and has managed international, regional and local business support projects, including research and development grant programmes and business growth initiatives. More recently, she has worked in the further and higher education sectors promoting the importance of skills development in driving economic productivity.

Dev Chakraborty: Gloucestershire LEP: Dev is currently the Deputy Chief Executive for GFirst LEP, Gloucestershire's Local Enterprise Partnership. Dev has over 25 years experience in marketing, sales and media roles in the South West, including 10 years of senior management and board level experience. Dev was part of the original team that launched Cornwall's award winning, commercial radio station, Pirate FM then becoming Managing Director of Star FM in Bristol. Immediately prior to his role at GFirst LEP he was a Business Guide at the Growth Hub working with high growth businesses across Gloucestershire.

Colette Mallon: Swindon and Wiltshire LEP: Colette leads Business Engagement for the SWLEP. She has specific responsibility for building relationships with businesses, government, stakeholder organisations and other LEPs to support the delivery of the Swindon and Wiltshire Strategic Economic Plan.

Annex E: Research Activity

This section sets out the tables and data unpinning the charts within Section 4.2 (Research Strengths).

Research activity

Table 7 Cyber Resilience Alliance-based organisations as project leads for publicly-funded research projects

	Projects led from the SIA	*% of UK projects*	*LQ*	*Value of projects led from SIA (£m)*	*% of UK funding*	*LQ*
Cyber Security	23	2.06%	2.22	1.64	0.39%	0.40
Data Science	36	0.54%	0.58	8.95	0.30%	0.31
All topics	**621**	**0.93%**	**--**	**283.83**	**0.98%**	**--**

Source: Technopolis Group, using Gateway for Research data and semantic text analysis powered by SpazioDati

Table 8 Cyber Resilience Alliance-based organisations as project leads for publicly-funded research projects

	Projects with participants from the SIA	***% of UK projects***	***LQ***	***Value of projects with participants from the SIA (£m)***	***% of UK funding***	***LQ***
Cyber Security	84	7.53%	1.26	61.52	14.81%	1.16
Data Science	537	8.08%	1.35	526.77	17.39%	1.36
All topics	**4,009**	**5.99%**		**3,700**	**12.78%**	

Source: Technopolis Group, using Gateway for Research data and semantic text analysis powered by SpazioDati

The following tables show the organisations in the Cyber Resilience Alliance area that have most frequently been involved in publicly funded research between 2007 and 2017. Duplicates may exist where organisations have bid under different names (which is sometimes the case where an organisation uses different subsidiaries to bid for public funding).

All topics:

Commented [DS3]: For appendix

The table below (related to Fig 6 in the report) shows the 50 SIA-based organisations with the most project participations across all research topics. As shown, research councils play a particularly prominent role. Together, the Medical Research Council, EPSRC and the Natural Environment Research Council account for 34% of the research projects participated in by SIA-based organisations. Furthermore, three other research councils (ESRC, BBSRC and AHRC) are amongst the ten most frequent participants in research projects.

The defence sector also accounts for fair share of project participations with Dstl and QinetiQ also being amongst the ten most frequent research project participants. Together they accounted for 8% of all the SIA area's project participations.

Figure 6: Top 50 organisations in SIA area by project participation across all topics

Rank	Name of organisation	Number of projects participated in	Overall value of projects participated in (£)
1	Medical Research Council	734	857,632,059
2	EPSRC	544	338,294,350
3	Natural Environment Research Council	345	168,408,100
4	Defence Science & Tech Lab DSTL	298	502,454,388
5	ESRC	262	165,556,758
6	BBSRC	261	159,343,837
7	Technology Strategy Board (now UKRI)	243	310,023,182
8	AHRC	210	98,766,957
9	Public Health England	85	120,490,480
10	QinetiQ Ltd	77	124,398,876
11	The Natural Environment Research Council	77	68,286,892
12	Renishaw Plc	69	161,406,147
13	Knowledge Transfer Network	54	168,516,929
14	STFC	53	31,023,957
15	Harper Adams University	47	17,709,226
16	GE Aviation Systems Limited	39	140,355,256
17	UK Space Agency	27	21,319,442
18	Campden Bri	21	31,515,780
19	RWE nPower	21	37,688,850
20	Renishaw P L C	20	25,726,071
21	Corin Group PLC	17	53,856,715
22	Teer Coatings Limited	16	6,962,605
23	Malvern Instruments Ltd	14	19,955,612
24	Innovate UK	13	14,556,906
25	RWE Generation UK Plc	13	8,436,715
26	Chronos Technology Limited	12	3,010,904

27	Teer Coatings Ltd	12	24,347,411
28	W R C Plc	12	20,150,533
29	Transport Systems Catapult	11	26,544,606
30	University of Gloucestershire	11	727,801
31	DairyCo	10	4,842,819
32	Intel Corporation (UK) Ltd	10	13,716,165
33	Safran Landing Systems UK Limited	10	44,921,234
34	The Pjh Partnership Limited	10	931,311
35	Agrii	9	3,577,599
36	Drisq Ltd	9	6,246,241
37	Smart Component Technologies Limited	9	2,091,984
38	Swanbarton Limited	9	11,659,711
39	AB Vista Feed Ingredients	8	1,965,965
40	Edf Energy Nuclear Generation Limited*	8	4,275,374
41	EDF Energy Nuclear Generation Ltd*	8	11,502,058
42	Gloucestershire Hospitals NHS Fdn Trust	8	16,903,193
43	Precision Varionic International Limited	8	2,167,780
44	RWE Innogy	8	15,362,819
45	Velcourt Limited	8	3,954,993
46	Grainger & Worrall Limited	7	34,304,620
47	Messier-Dowty Ltd	7	19,194,071
48	Progressive Energy Limited	7	5,199,296
49	University of Worcester	7	3,985,092
50	Velcourt Ltd	7	6,845,816

Source: Technopolis analysis of Gateway to Research data

** Separate entries in Gateway to Research database, repeated here verbatim*

Cyber security

As shown in Figure 7 in the report funding bodies account for many of the cyber security project participations by organisations based in the SIA area. Taken together, the Technology Strategy Board (which became Innovate UK, then UKRI), ESRC, AHRC, EPSRC, and Medical Research Council accounted for nearly half (48%) of all project participations in cyber security. Only three private organisations were involved in more than one publicly-funded cyber security projects: QinetiQ, PixelPin, and L-3 TRL.

Figure 7. SIA-based organisations that participated in cyber security projects

Rank	*Name of organisation*	*Number of projects participated in*	*Overall value of projects participated in (£)*
1	Technology Strategy Board	19	28,656,008
2	ESRC	12	11,259,790
3	AHRC	7	1,476,160
4	Defence Science & Tech Lab DSTL	7	7,367,941
5	EPSRC	4	602,518
6	Medical Research Council	4	1,314,869
7	Pixelpin Ltd	3	409,198
8	Qinetiq Ltd	3	6,267,888
9	Defence Communications Service Agency	2	458,235
10	L-3 TRL Technology	2	4,955,062
11	Alcatel-Lucent	1	276,977
12	Atg - It. Ltd	1	5,000
13	Azon Consulting Limited	1	5,000
14	British Computer Society	1	7,446,273
15	CESG	1	770,473
16	Chronos Technology Limited	1	370,363
17	Clickdebt Limited	1	5,000
18	Cuerden Consulting Limited	1	5,000
19	Deep-Secure Ltd	1	250,000
20	D-RisQ Ltd	1	1,304,454
21	Drp (UK) Limited	1	5,000

22	Eurolink Connect Limited	1	5,000
23	Fashion for Change Limited	1	5,000
24	Gbr14 Limited	1	69,168
25	Glacis Limited	1	5,000
26	Graffica Limited	1	5,000
27	Horizon Nuclear Power Services Ltd	1	4,153,664
28	Horus Security Consultancy Limited	1	5,000
30	Infinite Precision Ltd	1	50,522
31	Innova Engineering Limited	1	5,000
32	Intel Corporation (UK) Ltd	1	202,161
33	Knowledge Transfer Network	1	672,754
34	Malvern Cyber Security Cluster	1	3,662,582
35	Oem Partnership Limited	1	100,000
36	Poikos Limited	1	5,000
37	Public Health England	1	198,209
38	Quicksilva Limited	1	213,935
39	Rowanalytics Ltd	1	183,896
40	Stephen Hatfield	1	75,199
41	Swanbarton Limited	1	24,036
42	TrackwiSE Designs Limited	1	5,000

Source: Technopolis analysis of Gateway to Research data

Organisations collaborating with SIA-based research outfits

Analysing the organisations that participated in funded projects with Cyber Resilience Alliance-based researchers will help reveal more about the SIA area's reach, including with research-intensive institutions in neighbouring areas. The following tables shows the organisations that most regularly collaborated with SIA-based outfits over the period 2007 to 2017.

All topics

Figure 8 in the report shows the 50 organisations that have most frequently acted as collaborators with SIA-based firms across all topics. The list is dominated by higher education institutes with 19 organisations ranked 1-20 being universities. UCL, Imperial, Oxford and Cambridge, all institutions located within UK's so-called 'Golden Triangle' of science and technology, account for 7% of all collaborations. The SIA area's reach has also extended much further north with institutions like universities of Edinburgh and Manchester being amongst the most frequent co-participants.

Fig 8. The 50 organisations to have most frequently collaborated with SIA-based organisations – across all topics

Rank	*Organisation name*	*Number of grants that have co-participated with SIA organisations (2007-2017)*
1	University College London	478
2	University of Oxford	409
3	University of Cambridge	352
4	Imperial College London	317
5	University of Edinburgh	259
6	University of Manchester	242
7	University of Bristol	228
8	University of Nottingham	201
9	University of Birmingham	198
10	University of Southampton	191
11	University of Leeds	180
12	Newcastle University	180
13	University of Sheffield	162
14	King's College London	160

15	University of Glasgow	158
16	University of Warwick	137
17	Cardiff University	133
18	University of Liverpool	126
19	Dept for Env Food & Rural Affairs - DEFRA	120
20	University of Exeter	117
21	University of Bath	110
22	Queen Mary, University of London	105
23	University of York	99
24	Rolls-Royce plc	97
25	London Sch of Hygiene and Trop Medicine	94
26	University of Aberdeen	93
27	AstraZeneca plc	82
28	The Wellcome Trust Ltd	79
29	National Institutes of Health	78
30	The Scottish Government	76
31	The Wellcome Trust Sanger Institute	76
32	Heriot-Watt University	74
33	BAE Systems	73
34	University of Reading	69
35	National Physical Laboratory NPL	67
36	University of Dundee	65
37	University of Leicester	63
38	University of Strathclyde	62
39	Lancaster University	61
40	University of East Anglia	60
41	Cranfield University	59
42	Queen's University of Belfast	57
43	The Welding Institute	56
44	University of Surrey	54
45	Durham University	52

46	University of Sussex	51
47	Scottish Executive Env and Rural Affairs	51
48	Network Rail Ltd	51
49	Loughborough University	51
50	University of St Andrews	50

Source: Technopolis analysis of Gateway to Research data

Cyber security

As Figure 9 in the report shows, relatively few organisations had multiple collaborations with SIA-based researchers when it came to cyber security projects. Indeed, only 16 organisations had more than two co-participations with those based in the Cyber Resilience Alliance area. Again, universities were amongst the most frequent collaborators. Four (Oxford, Cambridge, UCL and Imperial) accounted for 8% of all collaborations with SIA-based organisations. In terms of private firms collaborating with the SIA area, Microsoft, BAE Systems and BT were all amongst the top ten co-participants. The three operate in different sectors (albeit that some operations may have some overlap), showing the cross-sectoral reach that the SIA area's cyber security organisations had.

Figure 9. The 50 organisations to have most frequently collaborated with SIA-based organisations – in cyber security

Rank	***Organisation name***	***Number of grants that have co-participated with SIA organisations (2007-2017)***
1	University of Oxford	9
2	University of Cambridge	7
3	University College London	7
4	Imperial College London	4
5	Microsoft Research Ltd	4
6	Cranfield University	4
7	BAE Systems	4
8	British Telecommunications Plc	4
9	Heriot-Watt University	3
10	University of Edinburgh	3
11	University of Strathclyde	3
12	Laing O'Rourke plc	3

13	BT Group	3
14	TRW Conekt	3
15	Arup Group Ltd	3
16	Newcastle University	3
17	Cisco Systems Inc	2
18	Intel Corporation	2
19	University of New South Wales	2
20	The Home Office	2
21	HP Research Laboratories	2
22	Thales Group	2
23	British Broadcasting Corporation - BBC	2
24	Symbian Software Ltd	2
25	KPMG	2
26	Swansea University	2
27	HW Communications Ltd	2
28	Royal Holloway, University of London	2
29	University of California, Berkeley	2
30	RED-M	2
31	University of Bristol	2
32	Queen's University of Belfast	2
33	Barclays Bank plc	2
34	Parsons Brinckerhoff Ltd UK	2
35	Laing O'Rourke	2
36	Ordnance Survey	2
37	King's College London	2
38	Orange Labs	2
39	University of Warwick	2
40	University of Manchester	2
41	HSBC Holdings plc	2
42	National Nuclear Laboratory Ltd	2
43	Zinwave Ltd	2

44	National Grid PLC	2
45	CPNI	2
46	National Crime Agency	2
47	Cardiff University	2
48	Motorola	2
49	University of Birmingham	2
50	University of Glasgow	2

Source: Technopolis analysis of Gateway to Research data

Annex F: Overview of Assets

Within this SIA, each of the LEPs provided information regarding their knowledge of local businesses and organisations involved with cyber security in the region. This was further developed by RSM (utilising Bureau van Dijk), and Technopolis. SIC codes were not utilised for this exercise given the breadth (SIC codes capturing Computing Activities will not best capture cyber security activities).

Firms were subsequently searched for within the region using Google Places – to provide co-ordinates for mapping the assets. We recognise that some of these firms are active in more than one location; however, have utilised a 'main location' to prevent duplication for analysis purposes.

Asset Type	Business name	Local Enterprise Partnership Region (Sourced using Google Places API)
Commercial Organisation	3SDL Limited	Worcestershire
Commercial Organisation	Advent IM	Black Country
Commercial Organisation	Airbus	Gloucestershire
Commercial Organisation	Anomali	Gloucestershire
Commercial Organisation	Anon AI	The Marches
Commercial Organisation	Ark Data Centre	Swindon and Wiltshire
Commercial Organisation	Ascentor Limited	Gloucestershire
Commercial Organisation	Assure Technical	Worcestershire
Commercial Organisation	Blockmark	Worcestershire
Commercial Organisation	Borwell	Worcestershire
Commercial Organisation	C2B2 Solutions	Worcestershire
Commercial Organisation	C3IA Solutions	Dorset
Commercial Organisation	Charlton Networks	Gloucestershire
Commercial Organisation	Chipside	Swindon and Wiltshire
Commercial Organisation	CIS Ltd	Thames Valley Berkshire
Commercial Organisation	Coinfirm Limited	The Marches
Commercial Organisation	Corvid	Gloucestershire

Commercial Organisation	Cyber Security Associates	Gloucestershire
Commercial Organisation	Cyberis Limited	Gloucestershire
Commercial Organisation	Cybertarge Consultancy Limited	Gloucestershire
Commercial Organisation	Cybsafe Limited	Swindon and Wiltshire
Commercial Organisation	D-RisQ	Worcestershire
Commercial Organisation	Deep Sky Blue Solutions	Gloucestershire
Commercial Organisation	Deep-Secure Limited	Worcestershire
Commercial Organisation	Dephrisk Limited	Worcestershire
Commercial Organisation	Distil Networks Limited	Gloucestershire
Commercial Organisation	Encription Limited	Worcestershire
Commercial Organisation	Exercise 3	The Marches
Commercial Organisation	Flatworld Works	Black Country
Commercial Organisation	Foregenix	Swindon and Wiltshire
Commercial Organisation	Fujitsu	London
Commercial Organisation	GBR14	Gloucestershire
Commercial Organisation	GE Aviation Systems Ltd	Gloucestershire
Commercial Organisation	Hardware Group Limited	Gloucestershire
Commercial Organisation	Herne Hill Consulting	Gloucestershire
Commercial Organisation	Hex Security Limited	The Marches
Commercial Organisation	Horus Security Consultancy	Oxfordshire
Commercial Organisation	Hypersonica Limited	Worcestershire
Commercial Organisation	IBM	Solent
Commercial Organisation	IMS Technology Services	Worcestershire
Commercial Organisation	Information Risk Management (IRM)	Gloucestershire
Commercial Organisation	Infosec People	Gloucestershire
Commercial Organisation	Innova Sec	Worcestershire
Commercial Organisation	Intel Corporation (UK) Limited	Swindon and Wiltshire

Commercial Organisation	Key IQ Limited	Worcestershire
Commercial Organisation	L-3 TRL Technology	Gloucestershire
Commercial Organisation	Lockdown Cyber Security Limited	Gloucestershire
Commercial Organisation	Lockheed Martin	Swindon and Wiltshire
Commercial Organisation	Logically Secure Ltd	Gloucestershire
Commercial Organisation	Madalorian Security Services	Enterprise M3
Commercial Organisation	Northrop Grumman	Gloucestershire
Commercial Organisation	OGL Computer Services Ltd	Worcestershire
Commercial Organisation	Orpheus Cyber Ltd	London
Commercial Organisation	OSPL	Worcestershire
Commercial Organisation	Outsource	Swindon and Wiltshire
Commercial Organisation	PixelPin	Gloucestershire
Commercial Organisation	PwC	West of England
Commercial Organisation	QinetiQ Ltd	Gloucestershire
Commercial Organisation	Raytheon UK	Gloucestershire
Commercial Organisation	Rift Technology Limited	Worcestershire
Commercial Organisation	Ripjar Limited	Gloucestershire
Commercial Organisation	RJH Technical Consultancy Ltd	Gloucestershire
Commercial Organisation	Sandettie Limited	Worcestershire
Commercial Organisation	Secure Systems & Technologies Limited	Gloucestershire
Commercial Organisation	Somerford Associated Limited	Swindon and Wiltshire
Commercial Organisation	Station X Limited	The Marches
Commercial Organisation	Stratia Consulting Ltd	Gloucestershire
Commercial Organisation	Surevine	Gloucestershire
Commercial Organisation	Tanium UK Limited	Gloucestershire
Commercial Organisation	The Friendly Nerd Ltd	Worcestershire
Commercial Organisation	The Missing Linq Ltd	The Marches

Commercial Organisation	Titania Ltd	Worcestershire
Commercial Organisation	Torchlight Group Ltd	Swindon and Wiltshire
Commercial Organisation	Total IA Limited	Gloucestershire
Commercial Organisation	TrustedIA	Swindon and Wiltshire
Commercial Organisation	Tyco Electronics	Swindon and Wiltshire
Commercial Organisation	VCW Security Ltd	The Marches
Commercial Organisation	Vysiion	Swindon and Wiltshire
Commercial Organisation	Wayra	Greater Birmingham and Solihull
Commercial Organisation	Xreach Limited	The Marches
Commercial Organisation	Zovolt Limited	The Marches
Business Park / Enterprise Zone	Cheltenham Cyber Park	Gloucestershire
Business Park / Enterprise Zone	Enigma Business Park	Worcestershire
Business Park / Enterprise Zone	Malvern Hills Science Park	Worcestershire
Business Park / Enterprise Zone	Skylon Park (Hereford Enterprise Zone)	The Marches
Public Body	AHRC	Swindon and Wiltshire
Public Body	British Computer Society	Swindon and Wiltshire
Public Body	Defence Fulfilment Centre	The Marches
Public Body	Defence Science and Technology Laboratory	Swindon and Wiltshire
Public Body	EPSRC	Swindon and Wiltshire
Public Body	ESRC	Swindon and Wiltshire
Public Body	GCHQ	Gloucestershire

Public Body	Gloucestershire Constabulary	Gloucestershire
Public Body	Innovate UK	Swindon and Wiltshire
Public Body	MoD Corsham	Swindon and Wiltshire
Public Body	STFC	Swindon and Wiltshire
Public Body	UK Space Agency	Swindon and Wiltshire
University	Bath Spa University	West of England
University	Coventry University	Coventry and Warwickshire
University	Cranfield University	South East Midlands
University	Harper Adams University	The Marches
University	Oxford University	Oxfordshire
University	University of Bath	West of England
University	University of Birmingham	Greater Birmingham and Solihull
University	University of Bristol	West of England
University	University of Gloucestershire	Gloucestershire
University	University of the West of England	West of England
University	University of Warwick	Coventry and Warwickshire
University	University of Worcester	Worcestershire
University	Wolverhampton University	Black Country
University	Wolverhampton University (Telford Campus)	The Marches
Training / Research / Representative Body	Corsham Institute	Swindon and Wiltshire
Training / Research / Representative Body	Cyber Security Training and Conference Centre at Berkeley Power Station	Gloucestershire
Training / Research / Representative Body	Cynam	Gloucestershire
Training / Research / Representative Body	IASME Consortium	Worcestershire

Training / Research / Representative Body	IoT Security Foundation	Worcestershire
Training / Research / Representative Body	Malvern Cyber Security Cluster	Worcestershire

Annex G: Case Studies

Business:

3SDL

3SDL is a leading defence and cyber data systems specialist, providing consultancy, services and training within the Defence and Security industry. Founded in 2005 and with headquarters in Malvern, cyber security is one 3SDL's core expertise with a team of specialists that support both government and business customers in identifying, prioritising, and addressing their cyber risks. Their services include threat assessments, design of technical solutions, cyber health checks, and the development of cyber security management plans including relevant training.

The company has engaged in a variety of collaborative activity with other cyber organisations in the SIA area. Working with other local cyber security firms, 3SDL is part of the membership organisation, Malvern Cyber Security Group. Consisting of around 40 other small cyber security firms, the members all co-operate with each other on initiatives to grow their businesses, to share practice, and improve cyber security. For instance, 3SDL worked with other Malvern-based companies Borwell, C2B2 and Deep Secure in developing a "dirty lab" research unit in Worcestershire to simulate attacks from hackers, and have a secure environment in which to test virus counter-measures.

3SDL's influence has also extended beyond the cyber sector, working with a number of local businesses to improve their cyber resilience. As part of the ERDF-funded Growing Cyber Project, Worcestershire based SMEs have been able to access two days free specialist cyber consultancy. Through this, 3sDL has worked with other local businesses, including Nature's Own, suppliers of nutritional supplements, to improve their cyber resilience. Specifically, 3SDL's cyber security consultants reviewed Nature's Own's IT infrastructure, helping them better understand their cyber security risks and how they could best be mitigated. Subsequently, 3SDL has helped Nature's Own obtain grants to fund cyber security improvements, as well as being named as Nature's Own's preferred cyber security adviser as part of a successful Innovation Voucher bid to the then Technology Strategy Board.

Publicly, 3SDL has alluded to there being several barriers to business growth. This includes the high local demand for individuals with cyber skills, with senior staff at 3SDL commenting how this presents staff recruitment and retention difficulties. This partly influenced 3SDL's decision to participate in the Malvern Cyber Apprenticeship Development Scheme (CADS). Run by 3SDL and QinetiQ, it provides sixth form students in Malvern Hills with 75 hours of innovative work place learning each year in the cyber security industry. 3SDL has viewed this as a way of nurturing the local talent pipeline, as well as giving something back to the community.

3SDL has highlighted other concerns too. This includes the lack of awareness by businesses (and therefore potential customers) of the dangers of cyber-attacks and protection mechanisms against them. Partly as a reaction to this, 3SDL has participated in cyber awareness events run by Worcestershire Business Central. The company has also spoken of government procurement processes being a constraint on growth. The Ministry of Defence's (MoD) procurement approach has been felt to be insufficiently lean, too slow, and too risk averse, making it much more difficult for small firms like 3SDL to win MoD contracts.

QinetiQ

QinetiQ is a British multinational defence technology founded in 2001. It has a major technology centre in Malvern, covering some 70 acres and with over 2,000 employees.[120] Malvern houses some of QinetiQ's cyber security operations both for corporate and government clients[121] and is a major player in the SIA area's cyber security cluster. In recent months, QinetiQ has recruited over 100 new staff at Malvern, in part to help service its growing cyber security business.[122] Although few public details are available about QinetiQ's project level collaborations with other cyber firms in the SIA area (potentially because of the sensitive nature of some of the firm's work), it is clear that QinetiQ is working closely alongside other cyber organisations in the area. For instance, QinetiQ is a partner and shareholder of Malvern Hills Science Park (MHSP) located adjacent to the firm's base in Malvern. MHSP is home to the National Cyber Skills Centre, and to a number of growing companies specialising in cyber security. The Park was established to help facilitate the spin-out of companies keen to exploit the commercial applications of military-focussed technologies developed at QinetiQ. A such, QinetiQ maintains working relationships with IT and cyber defence firms based at MHSP.[123]

QinetiQ's links with the local business community has also continued through the creation of numerous spin-off companies that have formed the cornerstone of the areas cyber security cluster.[124] Indeed, local stakeholders have likened QinetiQ to a "surrogate university," providing the area with considerable cyber skills and expertise.[125]

QinetiQ is also working with MHSP on the recently announced Worcestershire 5G testbed. Led by Worcestershire LEP and also involving MHSP, the testbed will focus on finding ways to increase productivity through 'preventative and assisted maintenance using robotics, big data

[120] Worcestershire Tourist Guides article, available at http://www.worcestershiretouristguides.com/Articles/Article_166.asp (accessed 3 May 2018)
[121] BBC News (2014) *Unlikely front line in the war on cybercrime*. Internet, available at http://www.bbc.co.uk/news/business-25726361 (accessed 3 May 2018)
[122] Malvern Observer (2017) *Malvern MP welcomes next generation of QinetiQ's graduates*. Internet, available at https://malvernobserver.co.uk/news/malvern-mp-welcomes-next-generation-of-qinetiqs-graduates/ (accessed 3 May 2018)
[123] UKSPA (date unknown) *Malvern Hills Science Park*. Internet, available at http://www.ukspa.org.uk/members/mhsp (accessed 3 May 2018)
[124] Kidderminster Shuttle (2013) *Malvern-based 'good guys' fighting back against cyber-crime*. Internet, available at http://www.kidderminstershuttle.co.uk/news/business_daily/10420436.Malvern_based__good_guys__fighting_back_against_cyber_crime/ (accessed 8 May 2018)
[125] Titania (date unknown) *Peter Day: 'Cyber Town Malvern'*. Internet, available at https://www.titania.com/about-us/news-media/peter-day%3A-'cyber-town-malvern' (accessed 8 May 2018)

analytics and AR over 5G.'[126] Entrepreneurs will be able to test 5G capabilities in a new commercial tech accelerator located at MHSP. Cyber security will play an important part in the testbed with QinetiQ bring brought into the project to advance their cyber security application, and to provide assurance on the 'security by design' of the new 5G and Internet of Things technologies.[127]

QinetiQ is also working with other organisations in the SIA area to develop cyber skills. In 2015, QinetiQ led the Cyber Security Challenge in collaboration with other organisations including the Cheltenham-based GCHQ. For the Challenge, QinetiQ and GCHQ (amongst others) designed a realistic and sophisticated simulated cyber-attach which contestants had to stop in real-time. Prizes included university bursaries, professional accreditation, and internships.[128] Working with Malvern-based 3SDL, QinetiQ has also run the Cyber Apprenticeship Development Scheme (CADS), encouraging students from Malvern schools to gain practical experience in cyber security.[129]

Publicly at least, QinetiQ has cited a skills shortage as being a notable barrier to the organisation's development. With cyber security being a growing and ever-increasingly important international issue, QinetiQ has highlighted a need to ensure that the right talent enters the industry in order to ensure the firm's future prosperity. A particular concern across the UK is a shortage of relevant talent and a lack of clear pathways from education to industry.[130]

BlackBerry Professional Cybersecurity Services (previously Encription UK)

Operating from a facility in Kidderminster, Worcestershire, BlackBerry operates a UK-based IT security arm that offers penetration testing, and IT security training courses for a mixture of public and private sector organisation. BlackBerry Cybersecurity Services was formed following BlackBerry's acquisition of the Kidderminster-IT security and forensics services company, Encription UK. The new firm continues to offer services round strategic security (e.g. cloud services), technical security (e.g. IT infrastructure) and detection, testing and analysis. As outlined below, Encription has for several years, engaged with other stakeholders in the SIA area on issues concerning cyber security and resilience.

Encription itself has named other cyber firms in Malvern as partners, most notably the software experts, Borwell, the cyber data systems firm, 3SDL, and Key IQ, one of the founders of the

[126] ISP review (2018) *Government Name Six UK Winners of £25m for 5G Mobile Trials*. Internet, available at https://www.ispreview.co.uk/index.php/2018/03/government-unveil-six-uk-winners-25m-5g-mobile-trials.html (accessed 3 May 2018)
[127] Ibid.
[128] SC Magazine (2015) *Country's largest cyber security organisations collaborate to design cyber-security challenge*. Internet, available at https://www.scmagazineuk.com/countrys-largest-cyber-security-organisations-collaborate-to-design-cyber-security-challenge/article/535282/ (accessed 3 May 2018)
[129] 3SDL (2018) *The Cyber Apprentice Development Scheme*. Internet, available at https://www.3sdl.com/news/cyber-security/about-the-cads.html (accessed 3 May 2018)
[130] SC Magazine (2015) Country's largest cyber security organisations collaborate to design cyber-security challenge

Malvern Cyber Security Cluster.[131] The extent of any commercial collaborations with these organisations is unclear but it is evident that Encription interacted with these organisations on a more informal and strategic level. They for instance worked alongside 3SDL and Borwell to found a 'dirty lab' in Malvern to test responses to viruses and cyber-attacks.[132] Encription is also a member of the Malvern Cyber Security Cluster with other local cyber firms such as 3SDL, D-RisQ (Malvern based defence software developers), IASME (Malvern based managers of an information security assurance standard), Titania (Worcester based security software firm) and Aurora Consulting (a Gloucestershire-based software engineering firm).[133]

Encription's most high profile collaborative activity has arguably been in the area of skills development, working with a range of local organisations and stakeholders on cyber skills programmes. For instance in 2013, working with 3SDL, Key IQ and Cheltenham-based QinetiQ, Encription helped to develop and deliver a series of free cyber security workshops for students in Years 9-11, held at the University of Worcester.[134] Through its involvement in the Malvern Cyber Security Cluster, Encription also launched the Cyber Academy, an employer-led work programme designed to inspire young people to consider cyber careers, provide them with relevant training, and provide new entry routes for them into the sector.[135]

Encription previously alluded to a key barrier to the cyber industry's growth being a lack of awareness from SMEs (and also a potential customer base for the firm) of the real risks presented by cyber-crime. As highlighted by Tony McDowell, the previous owner of the firm, SMEs have tended to assume that cyber-attacks and security breaches won't happen. However, as larger companies have installed more robust security measures, attackers have now tended to see SMEs as more viable targets. Furthermore, SMEs' awareness levels of what they can do to defend against cyber-attacks has often been poor too.[136]

[131] See Encription website, available at http://www.encription.co.uk/about-us/partners/ (accessed 8 May 2018)

[132] BBC News (2012) *Malvern 'dirty lab' to tackle cyber-crime*. Internet, available at http://www.bbc.co.uk/news/uk-england-hereford-worcester-17118464 (accessed 3 May 2018)
[133] Firetrench (2013) *Employer-backed Cyber Academy launched to boost UK's information security skills*. Internet, available at http://ftnews.firetrench.com/2013/08/employer-backed-cyber-academy-launches-to-boost-uks-information-security-skills/ (accessed 8 May 2018)
[134] University of Worcester (2013) *STEM Newsletter*. Internet, available at https://www.worc.ac.uk/documents/STEM_Schools_Newsletter_Autumn_2013v2_web.pdf (accessed 8 May 2018)
[135] Firetrench (2013) Employer-backed Cyber Academy launched to boost UK's information security skills
[136] Cited in Pierre Audoin Consultants (2013) *Competitive analysis of the UK cyber security sector*, p. 71. Internet, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf

Borwell

Malvern-based Borwell is a software company that specialises in bespoke secure software development and penetration testing to validate system security. Borwell also offers accredited one-day cyber security training courses to business professionals, giving them an insight into the dangers of cyber-crime and protection against it. Borwell is a central figure of the SIA area's cyber security cluster, maintaining a number of formal and informal links with other organisations in the area.

Borwell themselves have listed one of their partners as being the global security company, Northrop Grumman, who have a base in Cheltenham although they do not elaborate further on the nature of this relationship.[137] Borwell also has a particularly close relationship with fellow Malvern-based cyber firm, 3SDL, with the two firms having worked with each other on a number of commercial opportunities, bids, exhibitions, and several industry days.[138] Borwell and 3SDL's formal collaborations continued with their joint work on the development of UKCyberLab, Malvern's 'dirty lab' project for testing responses to cyber-attacks. The two companies jointly invested in the project[139] which has also involved other cyber organisations in the area. For instance, Kidderminster-based Encription was one of the facility's initial partners[140], while the development of the initial lab concept came about following discussion with cyber security experts at the Cheltenham-based GCHQ.[141]

Borwell also maintains some more informal links with other organisations involved in the wider cyber security cluster. Since its creation, the company has placed great emphasis on networking and working with other business in Worcestershire, viewing this as the only way of securing longer-term projects and to find the right talent needed for future growth.[142] Borwell is also a member of the Malvern Cyber Security Cluster, a collection of around 40 small cyber security firms, which co-operate with each other on initiatives aimed at growing their businesses, sharing best practice, and improving cyber security.[143]

Other high-profile projects with local stakeholders have centred on skills and training programmes. For instance, working alongside other organisations based in the SIA area including Key IQ (founders of the Malvern Cyber Security Cluster, and Malvern Instruments (suppliers of analytical instruments), Borwell has helped establish Code Clubs across primary and secondary schools in Malvern. Borwell has also worked alongside others in the delivery of cyber awareness

[137] Worcestershire LEP (2016) *Midlands Engine: Cyber Security Market Visit to Baltimore USA – Midlands, UK Delegate Profiles 18-2 October 2016.* Internet, available at http://www.wlep.co.uk/assets/FINAL-Midlands-Engine-GREAT_A4_Event_Brochure_Baltimore.pdf
[138] Based on a LinkedIn posting by director at Borwell.
[139] Borwell (2013) *Celebrating 10 years in business*. Internet, available at https://borwell.com/2013/02/03/celebrating-10-years-in-business/ (accessed 8 May 2018)
[140] LecLife (date unknown) *Invest in Worcestershire – Malvern Hills Science Park*. Internet, available at http://www.leclife.com/index.php?alec=search&qlec=Invest%20in%20Worcestershire%20-%20Malvern%20Hills%20Science%20Park (accessed 8 May 2018)
[141] Harriett Baldwin MP (2012) *MP tours ground-breaking 'Cyber* Lab'. Internet, available at http://www.harriettbaldwin.com/content/mp-tours-ground-breaking-'cyber-lab' (accessed 8 May 2018)
[142] Borwell (2013) Celebrating 10 years in business
[143] Kidderminster Shuttle (2013) *Malvern-based 'good guys' fighting back against cyber-crime*. Internet, available at http://www.kidderminstershuttle.co.uk/news/business_daily/10420436.Malvern_based__good_guys__fighting_back_against_cyber_crime/ (accessed 8 May 2018)

courses to local SMEs. For instance, working with Worcestershire County Council and Malvern-based cyber security software firm, Titania, Borwell ran an awareness course about the importance of cyber security in winning new contracts.[144]

Like other cyber firms, Borwell has previously spoken of a potential barrier to the sector's development being a lack of concern and interest by business owners (and therefore potential Borwell customers) in cybersecurity issues. In a 2018 interview, Borwell's founder spoke of how "business owners are still of the mind-set that they do not need to worry about online security."[145]

Universities:

Case Study: Universities in the region (within the Cyber Resilience Alliance)

The University of Gloucestershire, University of Worcester, and University of Wolverhampton offer cyber security specific courses at both an undergraduate and postgraduate level.

Recently, the University of Gloucestershire was announced as being a partner to the Institute of Coding which was highlighted by Theresa May within the 2018 World Economic Forum in Davos as being a key part of the Government's initiatives in reducing the digital skills gap[14].

One of the most popular courses offered by the University of Gloucestershire is the BSc Cyber and Computer Security degree[15]. The University of Gloucestershire also offers BSc Computer and Cyber Forensics[16] as well as a MSc Cyber Security[17] course; ultimately producing high quality graduates which local companies can utilise. These courses are supported by the University's Institute of Cyber and Risk Assessment whose applied research and knowledge exchange activities inform the teaching programmes and provide a basis of a service to business.

The University of Wolverhampton hosts a BSc Cyber Security course, from which 87% of graduates find full time employment or education within six months of graduation. The University recently (February 2018) secured £192,000 of funding to develop its cyber security course offer, including the development of a new MSc in Cyber Crime which will be designed to appeal to anyone with working experience in the area from entrance level up to established consultants and practitioners. It will be designed using CyberKombat - a cybersecurity modelling, development training, testing and certification environment which mimics real world security architectures and operations centres. The Wolverhampton Cyber Research Institute was also set up by the University in 2017 and aims to become a world leading multi-disciplinary Cyber Research Centre of Excellence, focusing on Secure Healthcare, Secure Transport

[144]FinditinWorcestershire (2018) *FinditinWorcestershire Breakfast Meeting: Be Cyber Secure to Win Contracts*. Internet, available at https://www.finditinworcestershire.com/events/finditinworcestershire-breakfast-meeting--be-cyber-secure-to-win-contracts (accessed 8 May 2018)

[145] Business & Innovation Magazine (2018) *Company Directors Lack Training in Responding to Cyber Attacks.* Internet, available at https://www.businessinnovationmag.co.uk/company-directors-lack-training-in-responding-to-cyber-attacks/ (accessed 8 May 2018)

including Automotive, Aviation and Secure Space; Secure infrastructure for sustainable cities; and Security for smart power grids.

The University of Worcester adds to this pool of graduates through its BSc (Hons) Computing course, covering a variety of skills applicable to Cyber Security operations directly.

Furthermore, universities in the region are expected to continue to invest in cyber security course and facility development in the coming years (see Section 5.4). The region is also expected to become host to the first brand new UK university in over thirty years – 'the New Model in Technology and Engineering (NMITE) which will focus on practical learning involving industry and public partners. It is expected to take 300 students in its first year (2018) but grow to 5,000 over the following decade and is expected to provide courses in cyber security.[146]

Public:

GCHQ: The Government Communications Headquarters (GCHQ) is a UK intelligence and security organisation that provides signals intelligence and information assurance to the government and security services. It is headquartered in Cheltenham with their site there being home to around 4,000 employees.[147] Sitting within GCHQ is the National Cyber Security Centre (NCSC), an organisation that provides advice to support to the public and private sector in how to avoid computer security threats. Some of the NCSC's operations take place at the Cheltenham headquarters, forming a central part of the SIA area's cyber security cluster.

GCHQ interacts with other firms in the SIA area in a variety of manners. Through the NCSC, GCHQ runs the Cheltenham Innovation Centre. This aims to support cyber security start-ups through the early months of business by providing a joint working environment for them to operate and collaborate in. Companies also have access to technical support from GCHQ.[148] The Cheltenham Innovation Centre is also home to The Cyber Accelerator which local firms are eligible for.

Elsewhere, the presence of GCHQ has helped encourage much larger firms to locate some of their research and development facilities to Gloucestershire in a bid to access the talent, facilities and opportunities that GCHQ can offer. For instance, in April 2015, Northrop Grumman opened

[146] New Model in Technology & Engineering, available at: http://nmite.org.uk/
[147] The Guardian (2003) *The Doughnut, the less secretive weapon in the fight against international terrorism.* Internet, available at https://www.theguardian.com/uk/2003/jun/10/terrorism.Whitehall (accessed 3 May 2018)
[148] National Cyber Security Centre homepage, available at https://www.ncsc.gov.uk/industry (accessed 3 May 2018)

a cyber centre in Gloucestershire to help deliver a large government contract for engineering services related to data security and information assurance, and also had a framework contract with GCHQ. Representatives from Grumman alluded to how the opportunity to collaborate with GCHQ formed a key driver for the Gloucestershire move, stating the location "will enable industry, customers partners and academia to collaborate in one location."[149] Similarly, a month earlier, Raytheon UK opened a cyber innovation centre in Gloucestershire for more than 100 engineers.[150] Seemingly, the close proximity to GCHQ and the opportunities this gives was a key driving force behind Raytheon's location choice.[151]

GCHQ has also collaborated and interacted with local institutions through its participation in different cyber skills programmes. For instance, the organisation previously ran Cyber Insiders, a Cheltenham-based cyber summer school that gave first or second year university students in subjects related to computer science, maths and physics a chance to learn from GCHQ's cybersecurity experts.[152] GCHQ has also previously run an apprenticeship scheme in collaboration with Gloucestershire College. During the three-year scheme, apprentices spend the first two years at Gloucestershire College learning the theoretical and technical skills needed. The third year involves a placement programme at GCHQ.[153]

The organisation has identified a couple of barriers to its continued development. The first concerns competition with the private sector for talent. Tech companies such as Google, Facebook, Microsoft and Amazon are able to offer much larger remuneration packages than GCHQ can, and do not have as stringent vetting processes for new recruits. Consequently, GCHQ has faced recruitment shortfalls in recent years.[154] GCHQ has also previously talked about it facing problems attracting a sufficiently diverse workforce, highlighting particular problems in attracting talented women to the cyber industry (currently women only account for 10% of the global cyber workforce).[155]

[149] Defense News (2015) *GCHQ Steadily Sparks UK Cyber Industry Rush*. Internet, available at https://www.defensenews.com/2015/04/14/gchq-steadily-sparks-uk-cyber-industry-rush/ (accessed 3 May 2018)
[150] Raytheon UK (date unknown) *Go Live; Raytheon Cyber Eco-system is UK First*. Internet, available at https://www.raytheon.com/uk/news/feature/go-live-raytheon-cyber-eco-system-uk-first (accessed 3 May 2018)
[151] South West Business (2015) *100 new jobs created as security business Raytheon opens new £3m cyber crime fighting centre in Gloucestershire*. Internet, available at http://www.southwestbusiness.co.uk/news/02022015081039-100-new-jobs-created-as-security-business-raytheon-opens-new--3m-cyber-crime-fighting-centre-in-gloucestershire/ (accessed 3 May 2018)
[152] GCHQ (2016) *Applications open for GCHQ's Cyber Sumer Schools.* Internet, available athttps://www.gchq.gov.uk/press-release/applications-open-gchqs-cyber-summer-schools (accessed 3 May 2018)
[153] Institution of Engineering and Technology (date unknown) *GCHQ advanced technical apprenticeship (electronics and electrical engineering)*. Internet, available at https://www.theiet.org/apprentices/meet-apprentices/company-case-studies/f-j/gchq-apprenticeship.cfm (accessed 3 May 2018)
[154] Financial Times (2017) *spy agency speeds up vetting in race for recruits*. Internet, available at https://www.ft.com/content/1fed299c-e72a-11e7-97e2-916d4fbac0da (accessed 3 May 2018)
[155] National Cyber Security Centre (2018) *Competition launches to crown UK's most cyber-savvy girls.* Internet, available at (https://www.ncsc.gov.uk/news/competition-launches-crown-uks-most-cyber-savvy-girls (accessed 3 May 2018)

Annex H: Methodological Considerations (LQs): (provided by Technopolis)

Throughout the SIA process Technopolis provided not only raw figures, but also some help in making sense of them. If the data sources allow, they do this through metrics and indicators that are normalised or referenced to different baselines or comparators. This can help the readers of the figures to make comparisons or to figure out if a particular data point is high or low with regards to a particular baseline.

For this, they usually provide the shares of particular metrics with respect to the national averages. For some data sources where they work thematically in addition to geographically, they try to go a bit beyond and provide another metric called the Location Quotient (LQ). LQs are used to try and abstract as much as possible the size of the object of analysis (in this case an SIA partnership region) and to give some indication on whether an activity (be it research and innovation funding, employment, patent output, etc.) is above or below an expected baseline/threshold.

Location quotients have been used in the past by the ONS and the ERC in the Witty review and the previous UK Industrial Strategy, using data of employment and number of companies, in order to work out areas of industrial and jobs concentration throughout the UK. It can be a bit tricky to unpack what the LQ conveys, because it is sometimes referred as a "concentration/specialisation" metric while in other occasions it is referred as "position over or under, relative to a baseline". These two explanations are compatible and come from the fact that you can write the formula for calculating the LQ in two (equivalent) ways (see formula below).

$$LQ = \frac{\frac{region_{theme}}{region_{all}}}{\frac{country_{theme}}{country_{all}}} = \frac{\frac{region_{theme}}{country_{theme}}}{\frac{region_{all}}{country_{all}}}$$

From the ERC's own paper Localisation of Industrial Activity across England's LEPs (which underpinned the LQs used in the Witty review): "Location Quotients are used to provide a broad illustration of the extent to which a particular activity is over- or under-represented [in a particular region] relative to the national average." [...] "If the LQ for an activity is less than 1, the [region] has a smaller share of [activity] than the GB average; if the LQ for an activity is greater than 1, the [region] has a larger share of [activity] than the GB average."[156]

At the same time, other definitions emphasise the "agglomeration" aspect. From NESTA's Creative Clusters and Innovation report: "Location quotients are a standard metric of agglomeration in economic geography that measure a given area's degree of specialisation in a sector, compared with the national average. A location quotient larger than 1 indicates that a particular sector is more important to the local economy than it is to the British economy."[157]

[156] Anyadike-Danes. M, et. al, *Localisation of Industrial Activity Across England's LEPs*. 2013. Available at: https://www.enterpriseresearch.ac.uk/wp-content/uploads/2013/12/RP15-LEP-Clusters-Report- Dec-2013-Final.pdf

[157] This definition is very close to the phrasing used in previous ONS papers and these NESTA reports are available at: https://www.nesta.org.uk/sites/default/files/creative_clusters_and_innovation.pdf
and https://www.nesta.org.uk/sites/default/files/summary_geography_uks_creative_high-tech_economies2015.pdf

Annex I: Funding

This annex sets out funding sources and commitments to the cyber security sector in the UK, underpinning Section 5.8 (Developments in wider funding landscape).

Department/ Public Body	Funding / Commitments to the Sector
National Cyber Security Centre (part of GCHQ)	The formal creation of the National Cyber Security Centre in October 2016 provided a hub of world-class expertise for businesses and individuals, as well as ensuring a clear vehicle for proactive and reactive response to major cyber incidents. When founded, it had a team of approximately 700 people[158]. It is part of GCHQ, which has an estimated 6,000 staff, the majority of which are based in the 'doughnut' building in Cheltenham. The aim of the NCSC is to make the UK the 'safest place to live and do business online'. It provides assistance to organisations across the UK, and monitors and tackles threats to national cyber defence. In 2017, it was particularly focused on tackling ransomware and distributed denial of service (DDoS) attacks, data breaches, supply chain compromises, and 'fake news' and information operations. The NCSC has invested in a number of initiatives to support and grow the businesses, skills, and embedding of cyber resilience throughout UK organisations, including: • **CyberInvest**: partnership that brings together key players from government and industry to invest and support the development of cutting-edge cyber security research across the UK's academic sector. To date, 24 companies[159] have committed to invest a minimum of £8m over the next 5 years. • **Industry 100**: Industry 100 brings together public and private sector talent to challenge thinking, test innovative ideas and enable greater understanding on cyber security. Industry 100 secondees work across a wide range of bespoke short-term placements at the NCSC normally on a part time basis. • **Cyber Security Body of Knowledge (CyBOK) Initiative:** Cyber Security Body of Knowledge has been set up with the long-term aim of contributing to the development of the cyber security profession. The project's purpose is to codify the cyber security knowledge which underpins the profession. Apart from giving structure to the core knowledge, topics and reference texts, the project - which is

[158] https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-09-04/7051/

[159] Airbus, BAE Systems, Becrypt, GSK, HP, HP Enterprise, Origone, Raytheon, Roke, BT, Cisco, Context IS, IBM, Leidos, Modux, SureVine, Thales, L3-TRL, Consult Hyperion, Crossword Cybersecurity, Cyberist, NCC Group, Nexor, Northrop Grumman, XQ Digital Resilience, QinetiQ.

	scheduled to run to July 2019 - will enable the UK to focus learning pathways, professional development and careers information. • **GCHQ Cyber Accelerator**: The GCHQ Cyber Accelerator is a collaboration between the UK Government Department for Digital, Culture, Media and Sport (DCMS), the Government Communications Headquarters (GCHQ), Wayra UK, part of Telefónica Open Future, and the National Cyber Security Centre (NCSC). Successful applicants will gain access to GCHQ's world-class personnel and technological expertise to allow them to expand capability, improve ideas and devise cutting-edge products to outpace current and emerging threats. The partnership will help teams develop their businesses and secure the investment needed to take their companies to the next level. A roster of best-in-class coaches and mentors from GCHQ and the wider Telefónica Group – including O2 and ElevenPaths – will provide support. Start-ups will also receive a financial grant, and access to work space.
Department for Digital, Culture, Media and Sport	"*We want to create a cyber ecosystem in which cyber start-ups proliferate, get the investment and support they need to win business around the world, to provide a pipeline of innovation that channels ideas between the private sector, government and academia.*" *The Rt Hon Matt Hancock MP, in National Cyber Security Strategy (2016-21)* The NCSS identifies funding gaps that exist in skills development, growth funding for SMEs, flexible funding models for research, and providing funding models to support forward-looking initiatives and technologies including: big data analytics; autonomous systems; trustworthy industrial control systems; cyber-physical systems and the Internet of Things; smart cities; automated system verification; and the science of cyber security. Since 2016, it has providing funding for several initiatives including: • **Cyber101:** Running nationally until March 2021, Cyber 101 is part of DCMS funded activity to grow the UK's cyber security industry and the capability of cyber security start-ups and scaleups. It is delivered in partnership with Digital Catapult, The Accelerator Network, CSIT and Inogesis. • **Cyber Security ICURe Programme:** The Innovation to Commercialisation of University Research (ICURe) Cyber Security Project is funded by the Department of Culture, Media and Sport (DCMS) and Innovate UK and is delivered through SETsquared.

	• **Cyber Schools Programme:** DCMS is investing £20m over four years to teach a comprehensive cyber security curriculum for almost 6,000 14-18 year olds each year.[160] • **Cyber Security Apprenticeships:** DCMS is promoting cyber security as an attractive career option as well as one that is vital to the UK's national interest. DCMS is also supporting leading employers in critical energy and transport infrastructure to train and recruit up to 50 highly skilled apprentices aged 16 and over to help defend essential services against cyber-attacks. The CNI cyber apprenticeships scheme is aimed at those looking to enter the cyber security profession and offers training in cyber security, as well as professional experience. • **Cyber Security Skills Intermediate Impact Fund:** The Cyber Skills Immediate Impact Fund pilot aims to increase the diversity and numbers of those working in the UK's booming cyber security sector. The Fund will incentivise a range of organisations develop, scale up, or refocus cyber security training initiatives. Value of the awards are in the range of £10,000 to £50,000 • **Infrastructure:** In line with the NCSS, DCMS has made a number of investments in supporting physical infrastructure complementary to the growth of the sector; for example, £15m in support for the National Innovation Centre for Data based at Newcastle University[161]; and £50m in support (2016-21)[162] for the Cyber Innovation Centres in London and Cheltenham. • **Policy Leadership:** In addition to funding, DCMS is actively pursuing policy development to support the rapidly moving sector, including supply and technology driven policies and initiatives e.g. Secure by Design[163], and demand side e.g. provision of the annual Cyber Security Breaches Survey to measure the costs and impacts of cyber threats.[164]
Department for Business, Energy, and	The UK Government's Industrial Strategy sets out a series of Grand Challenges to place the UK at the forefront of future industries including AI & the Data Economy, Clean Growth, Future of Mobility, and Ageing Society.

[160] GOV.UK, *Cyber Schools Programme.* 2017. Available at: https://www.gov.uk/guidance/cyber-schools-programme
[161] GOV.UK, *New national innovation centre to put UK at forefront of big data.* 2017. Available at:https://www.gov.uk/government/news/new-national-innovation-centre-to-put-uk-at-forefront-of-big-data
[162] GOV.UK, *Ground-breaking partnership between Government and tech start-ups to develop world-leading cyber security technology*. 2016. Available at: https://www.gov.uk/government/news/groundbreaking-partnership-between-government-and-tech-start-ups-to-develop-world-leading-cyber-security-technology
[163] GOV.UK, *New measures to boost cyber security in millions of internet-connected devices*. 2018. Available at: https://www.gov.uk/government/news/new-measures-to-boost-cyber-security-in-millions-of-internet-connected-devices
[164] Department for Digital, Culture, Media and Sport, Ipsos MORI Social Research Institute and University of Portsmouth, *Cyber Security Breaches Survey 2018: Statistical Release*. 2018. Sourced from Table 5.1. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Industrial Strategy	It recognises the UK's existing international strength in cyber security, and sets out its place as a priority business sector[165] Further detail regarding the Industrial Strategy and its commitment to the cyber security sector is set out within Section 4.3 of the report.
Department for International Trade	The Department for International Trade (and UK Export Finance) are key in supporting the ambitions of the UK's cyber security sector to grow its export base and promote the sector as highly attractive for investment at the international level. Set up in July 2016 (as an immediate response to the EU Referendum), DIT's remit is to secure 'UK and global prosperity by promoting and financing international trade and investment, and championing free trade.' **UK Cyber Security Export Strategy:** This Strategy identifies six of the 'most promising sectors for cyber security exports worldwide (Government, Financial Services, Automotive, Energy and Critical National Infrastructure, Healthcare and Infrastructure). It also sets out that UK cyber security companies are particularly strong in: • **Incident Investigation & Cyber Forensics** (Identification and Investigation of Cyber Security Incidents) • **Threat Intelligence collection, feeds and analysis** (monitoring and response to emerging threats) • **Cyber security certification and training** (systems to ensure strong information security and data protection) • **Vulnerability assessment and management** (identification of risks of cyber-attacks and development of response strategies) • **Professional services – supporting governance, compliance and regulation** The Cyber Exports Strategy sets out that DIT will support cyber security companies in the UK to pursue opportunities (through research, trade missions and meeting the buyer events), enable exports (through personalised support) and respond to market opportunities (through marketing, product development and support).[166] There are also other funding opportunities for cyber security firms through DIT, including but not limited to:

[165] HM Government, *Industrial Strategy: Building a Britain fit for the future*. 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf

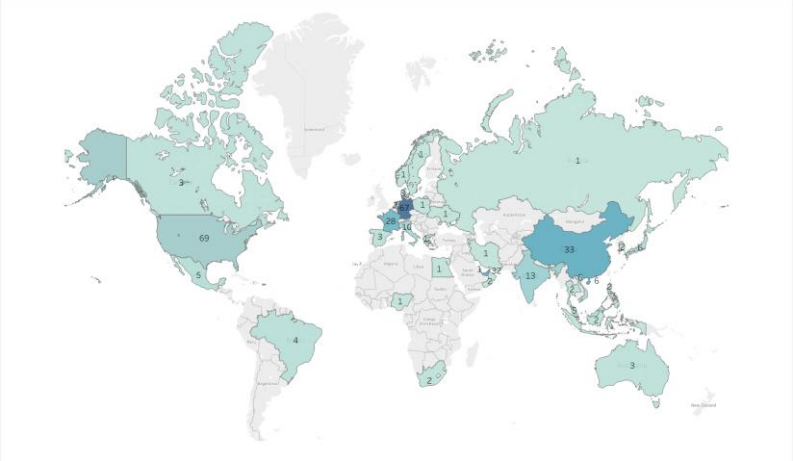
[166] https://www.gov.uk/government/collections/cyber-security-export-help

	DIT DSO: Department for International Trade Defence and Security Organisation (DIT DSO) helps cyber security organisations do more business internationally. **It helps UK companies to:** • increase their presence in overseas markets • overcome difficulties in getting into markets • develop supply chain opportunities • partner internationally in technology development • promote opportunities arising from prime contractor's supply chains, ideally at pre-bidding stage **through…:** • promoting the industry through trade envoys • promoting global export opportunities • working to match UK capability with opportunities • organising bespoke trade missions and other events helping companies to come into direct contact with buyers overseas • giving advice on particular overseas markets **Cyber Growth Partnership (CGP)** The CGP is composed of representatives from UK industry, government and academia; working in partnership to promote and create opportunities for UK cyber security companies. The CGP Exchange portal provides a focal point for cyber security businesses to engage, connect and collaborate and for non-cyber businesses to better understand cyber security and how to protect their business. **Cyber Demonstration Centre** **T**he UK Cyber Demonstration Centre (London) provides a location for the UK cyber security sector to showcase their products and services, and to help UK companies win more business overseas.

Tradeshow Access Programme:

The Tradeshow Access Programme provides funding in the form of grants for eligible businesses to attend overseas trade shows. The funding helps UK business gain:

- market knowledge
- experience in attending and getting the most from overseas trade shows
- advice and support from trade experts



Source: April 2018 – March 2019 – Upcoming Trade Missions (DIT, 2018)

Global Growth Pilot: ITI are about to launch the Global Growth Pilot, through which it will be seeking to specifically target ambitious businesses in the £5 million – £40 million turnover bracket to identify their barriers to export and provide support to overcome them through a co-investment model. It is hoped that the return on investment will be significantly greater than the current model. This will be tested over the next 12 months.

Great.gov.uk: ITI recently launched great.gov.uk, which is a world-leading platform developed by DIT to help UK businesses secure their place on the global stage by championing British goods and services overseas.

The platform is home to domestic and overseas-facing tools, including Export Opportunities, Selling Online Overseas, Find A Buyer / Find A Supplier and Invest in Great Britain.[167]

[167] Source: https://www.nao.org.uk/wp-content/uploads/2017/10/Short-Guide-to-the-Department-for-International-Trade.pdf

Cabinet Office	The Cyber and Government Security Directorate (CGSD) [168]supports Cabinet Office ministers in determining priorities in relation to securing cyberspace; coordinates the National cyber security programme and is responsible for Personal, Physical and Information Security Policy across government and internationally. The CGSD works with other lead government departments and agencies such as the National Cyber Security Centre (NCSC), GCHQ, Home Office, Ministry of Defence (MOD), the Foreign & Commonwealth Office (FCO) and the Department for Digital, Culture, Media & Sport. The CGSD is responsible for implementing a number of cross cutting agendas including: • to deliver the new National Cyber Security Strategy (NCSS) 2016 - 2021; • manage the five-year National Cyber Security Programme (NCSP) 2016 - 2021; • support the establishment of the National Cyber Security Centre (NCSC); • to continue to set policy for Government security; • implement the findings of the Government Security Review, seeking to transform the current security landscape through developing a new clusters model for Government.
Ministry of Defence	With National Offensive Cyber Planning allowing the UK to integrate cyber into all of its military operations, defence plays a key role in the UK's cyber security strategy. In Defence, the £800 million Innovation Initiative has boosted investment in UK research and business, with multi-million pound competitions to develop artificial intelligence and automated systems**.** A number of MoD initiatives, assets, and funding in cyber security are listed below: **Joint Forces Command – MOD Corsham** The United Kingdom Joint Forces Command (JFC), with its HQ's at MOD Corsham manages allocated joint capabilities from the three armed services it provides the foundation and supporting framework for successful operations by ensuring joint capabilities like information systems, cyber operations medical services, training and intelligence. MOD Corsham is home to the Global Operations Security Control Centre (GOSCC), the Joint Security Co-ordination Centre (JSyCC), Joint Forces

[168] GOV.UK, *Cyber and Government Security Directorate.* Available at: *https*://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

	Command's Information Systems and Services (JFC ISS) and the Cyber Security Operations Centre (CSOC). **Global Operations Security Control Centre (GOSCC)** Over £40 million has been invested in the new Cyber Security Operations Centre (CSOC), based at MOD Corsham, the investment is part of a wider government plan to invest £1.9 billion over five years to transform the MOD's operational cyber security capabilities. The CSOC works with the National Cyber Security Centre to facilitate the sharing of MOD cyber security challenges and contribute to wider national cyber security. The CSOC is a dedicated facility utilising state-of-the-art defensive cyber capabilities to protect the MOD's cyberspace from malicious attacks. **Information Systems and Services (ISS) -** the task of the ISS is information and communications technology support for MoD operations and business. ISS is responsible for information strategy and policy across the MOD and also the delivery of information technology systems across both the MOD's corporate and military elements. ISS employs in excess of 2,500 people and has a budget of more than £1.5 billion a year, with projects under development in excess of £10 billion in 2015. **Joint Forces Cyber Group** plans and co-ordinates UK cyber warfare operations. It commands Joint Cyber Units located at MOD Corsham and GCHQ Cheltenham and, the Joint Cyber Unit (Reserve) and Information Assurance Units. The Joint Cyber Unit (Reserve) was established in response to a growing cyber warfare threat and to allow the military to benefit from the expertise of civilian IT specialists. **Defence Academy of the United Kingdom** Based at MOD Shrivenham just across the Wiltshire border, Defence Academy provides higher education for personnel in the MOD, wider government, UK industry and overseas. They have links to 11 universities and provide a wide range of courses ranging from awareness up to expert level covering five broad course themes: leadership; command; technology; business skills; and international engagement. In March 2018, the MoD announced the opening of a new Defence Cyber School at the Defence Academy, Shrivenham. Part of a joint investment by the MOD and the National Cyber Security Programme, the School will address specialist skills and wider education in line with National Cyber Security Strategy objectives.

	Armed Forces' Minister Mark Lancaster, who opened the school, said: **"Cyber threats to the UK are constantly evolving and we take them very seriously. That's why the Defence Cyber School is so important. It's a state-of-the-art centre of excellence that will train more personnel across Defence and wider government in dealing with emerging threats."** The UK has advanced counter-cyber capabilities which can protect national interests from harm caused by adversaries. Furthermore, offensive cyber can be used to deal with serious threats to the UK.
Foreign and Commonwealth Office	The International Cyber Security Capacity Building Programme[169] aims to supply a portfolio of transformational projects to support the National Cyber Security Strategy and reduce the cyber threat to the UK. We invite concept proposals for projects to start in the financial year 2018 to 2019 and be completed by 31 March 2021, to help achieve the following objectives: •improve cyber security capacity in Eastern Europe, Association of Southeast Asian Nations (ASEAN), Middle East North Africa (MENA), India, Brazil or Mexico •promote a free, open, peaceful and secure cyberspace in Eastern Europe, ASEAN, MENA, India, Brazil or Mexico •conduct Cyber Security Capacity Reviews and help implement Active Cyber Defence (ACD) internationally
Department of Health and Social Care	In July 2017, the department published Your Data: Better Security, Better Choice, Better Care[170] in which it formally accepted the National Data Guardian's 10 Data Security Standards. Following WannaCry, the Digital Delivery Board (the governing board for the Personalised Health and Care 2020 programme which oversees better use of data and technology) reprioritised £21m capital for our major trauma centre hospitals and ambulance trusts. This funding is being used to upgrade firewalls and network infrastructure, and support the transition from outdated hardware and operating systems to improve resilience. These organisations were asked to undergo independent on-site assessments before applying for some of this funding which they could use to tackle high

[169] GOV.UK, *FCO Cyber Security Capacity Building Programme 2018-2021.* 2018. Available at: https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2018-to-2021
[170] GOV.UK, *New health data security standard and consent/opt-out model.* 2017. Available at: https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

	priority critical infrastructure vulnerabilities identified in their assessments. Trusts have now been allocated their share of the £21m. This funding is helping to build resilience by: • Upgrading firewalls to secure networks; • Minimising risk to medical devices i.e. MRI scanners and blood test analysis devices; • Supporting use of software to fix security vulnerabilities or upgrades for software applications and technologies (also referred to as "patching") by replacing obsolete PCs and introducing device security tools; and • Improving anti-virus protection. A further £25m of capital funding has been identified in 2017/18 to support organisations that have self-assessed as being non-compliant against high severity CareCERT alerts, strengthening hardware and software across the system. NHS Digital has secured an additional £4m to expand CareCERT services into an NHS Digital Security Operations Centre to improve monitoring of security threats, provide guidance and expert response to health and care organisations, and assure the public of the safety of their data. This will be operational from May 2018.[171]
Innovate UK	**Innovate UK provides businesses with support for cyber security and receiving Cyber Essentials certification:** Innovate UK is offering businesses Cyber Security Innovation Vouchers worth up to £5,000. They can use these vouchers to pay for an external expert to give them advice on protecting their business against cyber-attacks and potential accreditation to Cyber Essentials. They can also use this advice to protect new business ideas and intellectual property in cyber security. DCMS is also investing £500,000 in the new scheme with equal funding from Innovate UK.[172]

[171] Department of Health & Social Care, *Securing cyber resilience in health and care: A progress update.* 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678484/Securing_cyber_resillience_in_health_and_care.pdf

[172] Innovate UK Cyber Security (2018): https://www.gov.uk/government/news/cyber-security-apply-now-for-business-funding

	Further, IUK has recently established a Cyber Security Academic Start-ups Programme, which provides funding for individuals within a UK academic institution to support ideas that can be commercialised. **Successful applicants will participate in a 6-week programme (including three activities taking up to five days in London) to determine the value of the idea and, if appropriate, to identify the best commercial route to progress. The programme will be supported by industry experts, including those from cyber security. It will include the development of a detailed value proposition and an associated pitch. IUK plans to accept up to 30 applications.[173]**

Other Regional:

Initiative	Funding / Commitments to the Sector
Midlands Engine	The UK Government has pledged to invest £392 million across the Midlands through the Local Growth Fund. It will invest £20 million in a Midlands Skills Challenge to help close the skills gap between the Midlands and the rest of the country. In early 2017, the £250 million Midlands Engine Investment Fund was announced to finance the expansion plans of SMEs across the region. Further, the Midlands Trade and Investment Programme will help position the Midlands Engine on the global stage.[174] Digital technology, including in the cyber security clusters in Malvern and Nottingham, and the games development clusters in Leamington Spa and Coventry. Approximately 139,000 people are employed in the digital technology economy in the Midlands[175] **Midlands Engine Investment Fund** • MEIF's investment fund (£250m) is a collaboration between the British Business Bank, as well as ten Local Economic Partnerships in the East, South and West Midlands (The Marches and Worcestershire LEPs are included). • The MEIF has a vision to grow the local economy through the development of enterprise. Its aim is to fuel small businesses in the Midlands with the support of a range of investment instruments. • With support from the European Regional Development Fund, the Midlands Engine Investment Fund (MEIF) provides financial support

[173] http://researchfunding.sunderland.ac.uk/2018/01/17/innovate-uk-cyber-security-academic-startups-programme/
[174] Source: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/598295/Midlands_Engine_Strategy.pdf
[175] Office for National Statistics, (2016) *UK business register and employment survey.* Available at: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/businessregisterandemploymentsurveybresprovisionalresults/provisionalresults2016revisedresults2015

	to local businesses through instruments such as Small Business Loans, Debt Finance, Proof of concept and Equity Finance funds. • Its equity fund provides investments of up to £2m, with some allocated to <£250,000 in support of smaller businesses. • Its debt fund provides loans of between £100,000-£1.5m. Designed for more established companies, this investment instrument will help larger companies gain a foothold in the market. • Its small business loans fund is allocated to support smaller businesses in the Midlands region, with loans ranging in value of between £25,000-£150,000. • Its early stage / proof-of-concept fund is there to provide investments of up to £750,000 to test and develop new innovative ideas. With most equity loans dispersed across more mature businesses, proof-of-concept loans are essential in getting new businesses off the ground. • Recent MEIF funding case studies include a Nottingham-based firm, Solutions for Retail Brands, which provides cloud-based software and professional services to private brand retailers.

Appendix J: Certified Schemes

Certified Schemes

One essential process within the industry is testing products and services being offered to provide greater assurance to consumers of the overall validity of the product being offered. As such, there are several testing labs/facilities across the UK, providing CTAS and CHECK testing accreditations which identify any weaknesses utilising publicly known vulnerabilities and common configuration faults.

NCSC has released several certified product schemes which test the validity of cyber security products and services, providing greater assurance to consumers of the reliability and effectiveness of the products they purchase. There are several schemes within NCSC's oversight:

Commercial Product Assurance (CPA)

Commercial Product Assurance evaluates off-the-shelf cyber security products against security and development standards. Products which pass the assessment are given Foundation Grade certification, which is valid for two years. Developers are given a list of CPA Security Characteristics which can be used to instil confidence in consumers that they have traded in an NCSC-standard security product.

The assessments are carried out by NCSC-approved CPA Test Labs. These are:

- CGI IT UK Ltd – Reading, Berkshire
- Context IS - London
- DNV GL - London
- NCC Group - Manchester
- Roke – Romsey, Southampton
- KPMG - London
- BSI Cybersecurity and Information Resilience UK (Ltd) – Milton Keynes

Scheme fees - NCSC charge a fee for each certificate issued to cover the cost of their oversight of the process; **£4,690** paid by Test Lab to NCSC for each task.

Common Criteria (CC)

The Common Criteria Scheme is used to assure security-enforcing products, thus providing greater peace-of-mind as to the quality of the security features within the product's service offering.

The evaluations are carried out by Commercial Evaluation Facilities (CLEF) which charge a testing work fee to each provider being evaluated. The NCSC then charge the CLEF a fee for oversight of the accreditation process.

The NCSC evaluation CLEF partners are:

- DNV GL – London
- CGI IT UK – Reading

- BSI Cybersecurity and Information Resilience (UK) Ltd – Milton Keyes
- NCC Group – London
- Roke – Romsey, Southampton
- UL – Basingstoke, Hampshire

Scheme fees - NCSC charge a fee for each certificate issued to cover the cost of their oversight of the process; **£4,690** paid by Test Lab to NCSC for each task.

Commodity Information Assurance Services

Vendors are assessed by NCSC evaluation partners against pre-defined service requirements, and upon successful completion are certified by the NCSC. There are special circumstances in which the NCSC will both assess and certify; one example being services measured against the PKI CA Service Requirement.

The NCSC provides a list of all accredited vendors which have been evaluated by one of its evaluation partners:

- BSI Cybersecurity and Information Resilience (UK) Ltd – Milton Keynes
- KPMG - London
- NCC Group - Manchester
- Roke – Romsey, Southampton

Scheme fees - NCSC charge a fee for each certificate issued to cover the cost of their oversight of the process; **£5,505** paid by Test Lab to NCSC for each task, and **£20,810** for special circumstances such as evaluation of CAS-PKI CA.

Tailored Evaluation

Within the NCSC is the Tailored Assurance Service (CTAS) which provides assurance on the IT security components of a system, a product or a service. The accreditors have designed this in such a way which addresses questions posed by risk owners.

Tailored Evaluations are carried out by tailored assurance providers (professional services firms), including:

- CGI IT UK Ltd - London
- Context Information Security Ltd – London
- BSI Cybersecurity and Information Resilience (UK) Ltd – Milton Keynes
- IRM Ltd – Cheltenham
- KPMG – London
- NCC Group - Manchester

Scheme fees - NCSC charge a fee for each certificate issued to cover the cost of their oversight of the process; **£10,810** paid by Test Lab to NCSC for each task.

There are additional certifications awarded by the NCSC, although the scheme fees are less visible. These schemes see the NCSC conducting both the assessments as well as the certification processes, suggesting there are no evaluation partners and so fees are charged on a case-by-case basis to cyber security vendors seeking accreditation.

CAPS Assisted Products

CAPS evaluate products which facilitate the control of data flow between domains of differing classifications, but primarily it evaluates cryptographic products which provide security. CAPS has been launched as an amalgamation of knowledge sharing between the NCSC's the National Technical Authority for Information Assurance and the private sector to grow the number of High Grade products.

Developers are able to utilise NCSC cryptographic or public domain algorithms within their products. Once companies have access to NCSC knowledge and experience in Information Assurance, developers put forward their products for evaluation by the NCSC. Once certified, these products are then listed on the NCSC Approved products list.

TEMPEST and Electromagnetic Security

TEMPEST and EMS services help companies to understand how vulnerable their ICT system are to unintentionally release classified information and helps to ensure that appropriate countermeasures are in place.

The NCSC offers Operational Assurance and Consultancy Services and training. They also certify products and platforms to reassure UK government customers that the products' TEMPEST integrity lasts the lifetime of the product. The NCSC has accredited test facilities for certifying products (CFTCS):

- QinetiQ – Farnborough, Hampshire
- Secure Systems & Technologies Ltd - Gloucester
- TUV Product Service Ltd – Fareham, Hampshire

And, platforms (CPTAS):

- QinetiQ – Farnborough, Hampshire
- AugustaWestland – Yeovil, Somerset
- Malvern Optical – Worcestershire
- Secure Systems & Technologies Ltd - Gloucester
- TUV Product Service Ltd – Fareham, Hampshire
- RAF Waddington TEMPEST Test Team – Lincolnshire

Cyber Security Incident Response Scheme

Approved by the Council of Registered Ethical Security Testers (CREST), the scheme focuses on enforcing standards for incident response suited to industry, the wider public sector and academia.

Endorsed by the NCSC and CPNI, the CSIR CREST scheme delivers assurance as to the effectiveness of their cyber security incident response services.

Appendix K: Sector Potential

The economy of Shropshire, Herefordshire and the Marches has a particular focus on agriculture. 85% of land in Shropshire and 84% of land in Herefordshire is devoted to agriculture and over 6,300 farm holdings across the Marches area. The region has more people employed in Agri-Tech than any other LEP area. The sector nationally supports 3.8 million jobs and contributes £96 billion to the UK economy. Key agri-food companies within the Marches LEP include McConnel, the world leader in Vegetation Maintenance, Remote Control Technology, Cultivation & Seed Drills which is based in Ludlow and Fullwood, a world leader in robotic milking parlours, which is based in North Shropshire. Other significant businesses in this sector include: GKN Land Systems in Telford and both JCB and Jaguar Land Rover in our neighbouring LEP.

Harper Adams University is a key asset for the Agri-Tech industry in the Marches. It is the leading UK institution specialising in agriculture and agricultural engineering, as well as being an internationally recognised Centre of Excellence in this sector. It boasts a £2.93m Agricultural Engineering Innovation Centre based at the National Centre for Precision Farming and a multi-million pound research programme on precision agriculture, robotics and unmanned vehicles. Nearby Keele University, in our neighbouring LEP, offers a complementary Sustainability Hub. In 2016, it received a share of £1.7 million in government funding to run two new engineering conversion courses, specifically in Automotive Engineering and Agricultural Engineering. This is part of a broader drive to develop engineers to meet the future needs of employers, which include 'data science, cybersecurity, and software engineering'.[176]

There have been a number of innovations in the agri-food/tech sector that are vulnerable to hackers. The industry has moved away from paper trail information and depends more and more on new digitised technology. Advanced sending and monitoring technology means there is increasing use of the Internet of Things and use of third party data. Many aspects of agri-food today produce large amounts of data that need to be secured. Software is a key part of agri-digital infrastructure and if these are not kept completely updated then they continue to be vulnerable. This relies on human input and is therefore prone to human error.[177]

Hackers could use weak security in industrial control systems to exploit the agri-food/tech sector. Cyber security experts have warned that ransomware, or malicious software demanding cash payments, could force companies to choose between damaging downtime or paying a ransom to a hacker. Ransomware has expanded the number of potential attackers who could be interested in targeting critical infrastructure, from nation states and hacktivists trying to cause destruction, to

[176] Harper Adams University, Harper *Adams receives share of £1.7m to start engineering conversion courses*. 2016. Available at: https://www.harper-adams.ac.uk/news/202805/harper-adams-receives-share-of-17m-to-start-engineering-conversion-courses

[177] Capgemini Consulting & Wageningen UR (University & Research centre), *Cybersecurity in the Agrifood* sector. 2016. Available at: https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/02-029.16_agrifood_pov_consulting_web.pdf

those motivated by financial gain. Ransoms have been increasing as 70 per cent of companies pay those demanded, according to research by IBM.[178]

Ransomware has previously been used to halt production at agri-food plants. A Cadbury's chocolate factory in Hobart was forced to stop after a successful ransomware cyberattack. This was the result of a 'Petya' ransomware attack, which infected computers displaying a message demanding $300 worth of bitcoin.[179]

Autonomous Vehicles:

Autonomous vehicles are a key area of growth that could be vulnerable to cyber security issues. These are vehicles that can sense the environment and navigate without (or with limited) human input. These operate using radar, laser light, GPS, odometry and computer vision.

Jaguar Land Rover has considerable presence adjacent to the SIA region. Five of their six UK locations are based in the West-Midlands which include in Birmingham, Coventry, and Wolverhampton. The Wolverhampton location is the only location to be situated within the SIA however. UK Jaguar Land Rover's Wolverhampton base, The Engine Manufacturing Centre, was opened in 2013 and employs nearly 1,400 people. It is the first time Jaguar Land rover has designed and specified their own British production facility. Manufacturing a range of Jaguar Land Rover petrol and diesel engines, the plant consciously places engine supply close to production facilities.

Jaguar Land Rover have announced plans to help in the production of self-driving cars. Jaguar Land Rover plans to create a fleet of more than 100 research vehicles over the next four years. Data sharing between vehicles would allow future connected cars to co-operate and work together to assist the driver and make lane changing and crossing junctions easier and safer. The research project will test a number of technologies including; Safe Pull-away, helping to limit low speed collisions, Over the Horizon Warning, testing devices that use radio signals to transmit relevant data from vehicle to vehicle.

In addition to the above, Over the Horizon Warning is part of a research project testing devices that use radio signals to transmit relevant data from vehicle to vehicle. If vehicles were able to communicate independently, drivers and autonomous cars could be warned of hazards and obstacles over the horizon or around blind bends and finally emergency vehicle warning allows connected ambulances, police cars or fire engines to communicate with other vehicles on the road.

Jaguar Land Rover plans to supply up to 20,000 of its new electric I-Pace cars to Waymo, to be converted into self-driving vehicles for its ride-hailing service. This is a vehicle which was designed and engineered from its research and development facility in the West Midlands. Waymo is currently the only company with a fleet of fully self-driving cars and plans on launching the first robotic taxi service.

---

[178] Financial Times, available at: https://www.ft.com/content/81c01028-73a6-11e7-aca6-c6bd07df1a3c

[179] The Guardian, *Petya cyber-attack: Cadbury factory hit as ransomware spreads to Australian businesses*. 2017. Available at: https://www.theguardian.com/technology/2017/jun/28/petya-cyber-attack-cadbury-chocolate-factory-in-hobart-hit-by-ransomware

The Government wants to build new experimental roads in the West Midlands which are designed specifically for driverless cars. This was revealed in the Government's Industrial Strategy, and is part of a plan to see UK companies at the forefront of autonomous vehicles. £150 million is available for firms, including JLR, to test autonomous vehicles on public roads by 2021. A £5m trial to test 5G applications. and deployment on roads in 2018, will help to test how we can maximise future productivity benefits from self-driving cars, building on the work already progressing on connected and autonomous vehicle trials in the West Midlands. The first of Jaguar Land Rover's fleet of over 100 research cars will be driven on a new 41 mile test route on motorways and urban roads around Coventry and Solihull throughout 2016.

With the increase in use and investment in autonomous vehicles comes with it greater risks of cyber security threats, especially given the nature of how autonomous vehicles function. In its most basic form, car hackers find ways into vehicles through connections to the outside world. With the increase of use of self-driving cars comes an exponential increase in the number of connections these cars need to make given the network of devices they work with, such as traffic lights and junctions. It is possible for remote hackers to gain direct control over the vehicle.[180] The expertise within the Cyber Resilience Alliance region will provide direct research and commercial opportunities to address these vulnerabilities directly.

Advanced Manufacturing:

Across the region, advanced manufacturing plays an important role. Within the Marches LEP, manufacturing accounts for 14.1% of all employment and 36,700 people are employed in a manufacturing relevant occupation. There are a number of polymer companies within Telford, such as Bischof & Klein, Cedo UK, Craemer Environmental Systems and Smithers RAPRA. Automotive manufacturing employs 3,400 people in the region.

The scope of Advanced Manufacturing covers opportunities for research, development, prototyping and practical application in the areas of Advanced Materials, Innovation and Vehicles. The University of Wolverhampton's Telford Innovation Campus, located next to the main business parks of Telford, currently houses: Research; Business Engagement; Process & Product Development; Education; CPD and training activities. It is home to 300 students studying engineering-based courses as well as approximately 50 businesses. Approximately £12m is currently being invested in the campus to create new state-of-the-art facilities and courses to help create the next generation of skilled engineers in response to the regional and national shortage of qualified engineering graduates.

Worcestershire has an automotive supply chain, linking with Jaguar Land Rover and other car manufacturers. Machine manufacturing and engineering employment is approximately 85% above the England average per capita.[181] **Yamazaki Mazak is the world's largest producer of computer controlled metal cutting machine tools,** encompassing everything from jewellery to jet engines. The company's European Head-quarters and its UK base are in Worcester, which houses one of the most advanced manufacturing plants in Europe and employs over 400 people.

[180] Financial Times, available at: https://www.ft.com/content/6000981a-1e03-11e8-aaca-4574d7dabfb6
[181] Worcestershire Local Enterprise Partnership, *Advanced* Manufacturing. Available at: http://www.wlep.co.uk/about/worcestershire/about-wlep/growth-sectors/advanced-manufacturing/

Adjacent to the region, The University of Birmingham has an Advanced Manufacturing Technology Centre, with key partner Rolls Royce, and this specialises in practical applications, manufacturing development, problem solving and improving competitiveness.

Technologies utilized to drive the business are likely to include complex global networks, a myriad of back office business applications, generations of different industrial control systems (ICS) controlling high-risk manufacturing processes, and a variety of technologies directly embedded into current and emerging products. Deloitte and MAPI (Manufacturer's Alliance for Productivity and Innovation) research that numerous organisations have increased their cybersecurity budget due to a lack of awareness from the top-down. Whilst many respondents believed that IP threat was the main reason they were being targeted, many organisations had not taken the correct precautions for this. The majority of participants relied exclusively on internally conducted cyber risk assessments. Nearly half of the companies surveyed have connected products to that both stores and transmits confidential data. Finally, many of those surveyed are only beginning to understand the cyber risks to their businesses rather than them being a secure, modern digital environment.[182]

In response to security concerns, Mazak has partnered with CISCO to develop the SMART BOX cyber security system. The SMART BOX provides cyber security protection allied to analytical insight, including access to live data streams in cycle, feed rate reports and completion reports. The SMART BOX system can monitor data from any machine regardless of manufacturer, age or CNC.[183]

[182] Deloitte & MAPI, *Cyber risk in advanced manufacturing*. 2016. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manufacturing-cyber-risk-in-advanced-manufacturing-executive-summary.pdf
[183] Mazak, available at: https://www.mazakeu.co.uk/industry4/maintenance/