CYBER & DEFENCE IN THE MIDLANDS

The economic power of Midlands clusters

MIDLANDS CYBER

The Cyber Cluster for the **West Midlands**

MIDLANDS ENGINE

APRIL 2025

Contents

Purpose

This report is the result of an extensive roundtable discussion involving more than 50 leaders from industry, government and academia involved in the cyber and defence industry. It aims to characterise the sector in the Midlands from an investment perspective, highlighting the region's key strengths, opportunities and challenges, and builds upon the robust analysis of business and academic activity in the Investment Potential of Midlands Clusters reports.

By presenting this comprehensive analysis, this report seeks to support policymakers, businesses and local growth entities in promoting the Midlands as a leading hub for cyber and its defence applications and attracting prospective investors. A list of the organisations involved in this exercise can be found in the Appendix.

Executive summary

There is a thriving ecosystem of cyber and defence activity in the Midlands, with several major business and innovation hubs connected through MOD-linked cluster organisations adjacent to major cyber security and military assets such as the RAF Waddington and GCHQ. Beyond this there is a significant traditional defence manufacturing footprint across automotive, aerospace and submarine capabilities and leading university research centres and demonstrators. The region is well-positioned to drive technological advancement, strengthen national security and attract both global and domestic investment.

Key strengths

Leading cyber and defence hub: the Midlands is the largest cyber and defence cluster outside London and the Greater South East, contributing over £5bn GVA[1]

Strong workforce and military presence: Home to 13,000 cyber security professionals and 34,850 defence and security personnel, with major armed forces hubs

Cross-sector innovation: cyber security capabilities as well as integration across key industries, including aerospace, automotive, space and advanced manufacturing

Government and industry collaboration: Established clusters such as Midlands Cyber, and the Three Counties and Greater Lincolnshire Regional Defence and Security Clusters drive innovation and regional competitiveness

Innovation Ecosystem: leading business and technology parks and laboratories, including UK Telecommunications Laboratory, MIRA Technology Park, Malvern Hills Science Park, Manufacturing Technology Centre, Skylon Park, and Lincoln Science and Technology Park.

World-Class Academic and Research Assets: 59 cyber/defence focused research centres and training programmes across multiple universities.

Strategic Defence Sites: home to key end-user sites such as RAF Waddington and proximity to GCHQ.

Dual-Use Opportunities: Viable innovations for both defence and adjacent industries, such as medical imaging and autonomous mobility.

Significant portion of Cyber Valley: The UK's largest concentration of cyber businesses outside London.

Challenges

Funding barriers: Many SMEs struggle to access grants and investment due to closed supply chains, lack of private finance options in the Midlands, and defence applications being excluded from some funding schemes

Talent shortages: A limited pipeline of skilled cyber security professionals, particularly in defence and engineering-related roles

Regulatory gaps: Existing cyber security regulations have not kept pace with technological advancements

Awareness: The Midlands' cyber and defence strengths need greater local, national and international promotion.

1. Cyber security sectoral analysis 2025 - GOV.UK

Growth opportunities include:

Complete supplier-to-end user 'ecosystem' with extensive business support capacity: a compelling case for locating cyber and defence-oriented business expansion

Specialisation over generic competition: specific strengths in areas such as mobility, quantum, manufacturing and 5G utilisation

Securing the defence supply chain: leading new standardisation and addressing supply chain security weaknesses

Government support and defence innovation funding: significant funding availability such as NATO's DIANA €1bn fund

Building a connected cyber and defence ecosystem including adjacent industries: better connecting several major clusters for a pan-regional cluster & stronger value proposition

Strategic asks include:

Further professionalise cyber security to strengthen defence supply chains: accreditation and regulations that keep pace with industry and capability requirements, with standardisation increasing accessibility for new entrants

Secure long-term funding and clear policy: Establish more comprehensive and accessible funding support for SMEs, promote accreditation schemes and enforce security standards

Expand international collaboration and market access: access to European rearmament presents a significant opportunity to UK suppliers

Drive talent and workforce development: Flexible apprenticeship models at all levels and fast-tracking security clearance processes

Work to address cyber and defence industry profile and perceptions: both public understanding of career opportunities and wider public relations – the importance of sovereign defence capability to everything

Connect and promote the Midlands as a cyber and defence innovation hub: increased concierge role in established clusters to promote region's capabilities

The Midlands' cyber and defence clusters are major components in the UK's sovereign defence capability, with significant strengths in industry, research and development, software development and and advanced manufacturing. By tackling the challenges and capitalising on the opportunities outlined in this report, the region can further establish itself as a national leader in cyber-resilience and defence. Strategic investment, targeted policy support and stronger collaboration between government, industry and academia will be essential to unlock the full potential of this high-growth sector.

Why cyber and defence?

This report focuses on the transect between the cyber and traditional defence sectors: cyber and digital capabilities in security: from network resilience to software fundamental to physical defence functionality, as well as across defence manufacturing supply chains. Cyber is more than just software technology, encompassing the processes and skills to make decisions and understand data.

UK and European defence spending is set to significantly increase in the coming years with a focus on rearmament, and uncertainty around long-held alliances highlights the need to maintain sovereign capability across the defence supply chain. Cyber security is integral to these ambitions, as well as national security more broadly (the UK received 4million cyber attacks in 2024, of which 400,000 were successful). Existing defence contracts are extensive in the Midlands, with the Ministry of Defence alone procuring £3bn of work in 2024.

With the Midlands is home to a network of internationally significant business and innovation assets and capabilities (both current and nascent) that underpin this cyber and defence growth opportunity, this report sets out to showcase these capabilities in the region.

Although the Midlands Engine is closing in July 2025, a separate project in partnership with the Manufacturing Technology Centre and Ministry of Defence is looking at the economic impact (and growth potential) of the defence industry in the Midlands, focusing on advanced manufacturing as well as cyber applications like AI and Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) capabilities, in line with the Defence Industrial Strategy.

The Midlands' cyber and defence cluster

The Midlands is home to an established ecosystem of cyber and defence businesses, leading Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) capabilities, along with multiple internationally significant innovation hubs in this area such as the UK Telecoms Lab, Manufacturing Technology Centre, and MIRA Technology Park and new assets such as the University of Warwick's Internet of Things Security Operational Test and Evaluation Centre – the UK's first end-to-end security and resilience test lab for Internet of Things applications.

Existing defence applications and new dual use opportunities may be found across the cyber & defence sectors as well as adjacent sectors with significant footprints in the Midlands: advanced manufacturing, aerospace, space, and automotive, as well as sub-sectors such as medical imaging, demonstrating opportunities to pivot into defence markets. Cyber security applications play a crucial role in defence, with a growing need to enhance cyber-resilience.

Parallel reports on the aerospace and space technologies clusters highlights the Midlands as one of the world's most significant aerospace hubs, boasting over a century of expertise in production and research and development.

The Midlands also leads the UK's automotive manufacturing sector, producing one third of all UK cars and one quarter of its engines, with leading cyber and automotive innovation hubs and initiatives such as Midlands Future Mobility and Connected and Automated Mobility projects, with many transferable opportunities for defence applications. These overlapping industries already have established Tier 2 and 3 supply chains.

Collaboration across sectors that can drive innovation (which may generate dual use opportunities) is a major opportunity in the Midlands. However standards required for military use are far higher than civilian requirements, and so dual use opportunities may require extra support to develop to meet these requirements. An example of this cross-sectoral innovation in practice can be seen at **MIRA Technology Park**, which has transitioned from a purely automotive focus to complementary specialisations in air, marine and cyber among others.

Business and investment

Over 600 businesses headquartered in the Midlands have activities in the cyber and defence space[2] of which nearly 80% are SMEs, with hundreds more operating in the region. These Midlands enterprises generate an estimated £3bn in gross value add (GVA) and accounting for 15% of the UK's cyber and defence business registrations.

Major cyber and defence company sites in the region, include Specialist Computer Centres (SCC), GCHQ, Telent, Intertek, SRC UK, Meggitt, Rheinmetall BAE Systems, Rolls Royce, EDF Arabel, NP Aerospace, Moog UK, NMS, Collins Aerospace, and GE Vernova. Beyond these, there is a thriving network of SMEs such as Metrea Mission Data, Nettitude, Spectra, and Goldilock.

While cyber-focused businesses are arguably less 'sticky' to a place than other business activities, requiring little physical infrastructure to operate, the extensive support system in the Midlands as well as full supply chain from innovation hub to end-user military bases creates a unique regional (to global) market poised for growth.

As can be seen in the map overleaf, there are notable concentrations of these businesses in Telford, Birmingham and Warwickshire, Derby, Nottingham, Lincoln and Worcestershire. Many of these are in key business parks or innovation sites such as **Malvern Hills Science & Technology Park** (Herefordshire), the **Manufacturing Technology Centre** (Antsy), and Lincoln Science and Innovation Park.

This is corroborated by the government's own Cyber Security Sectoral Analysis 2025[3], which found that 10% of the UK's cyber security employment is in the Midlands: 3% being in the east of the region, 7% in the west). The region is also home to 8% of the UK's sites (3% East, 5% West), with concentrations in the same places.

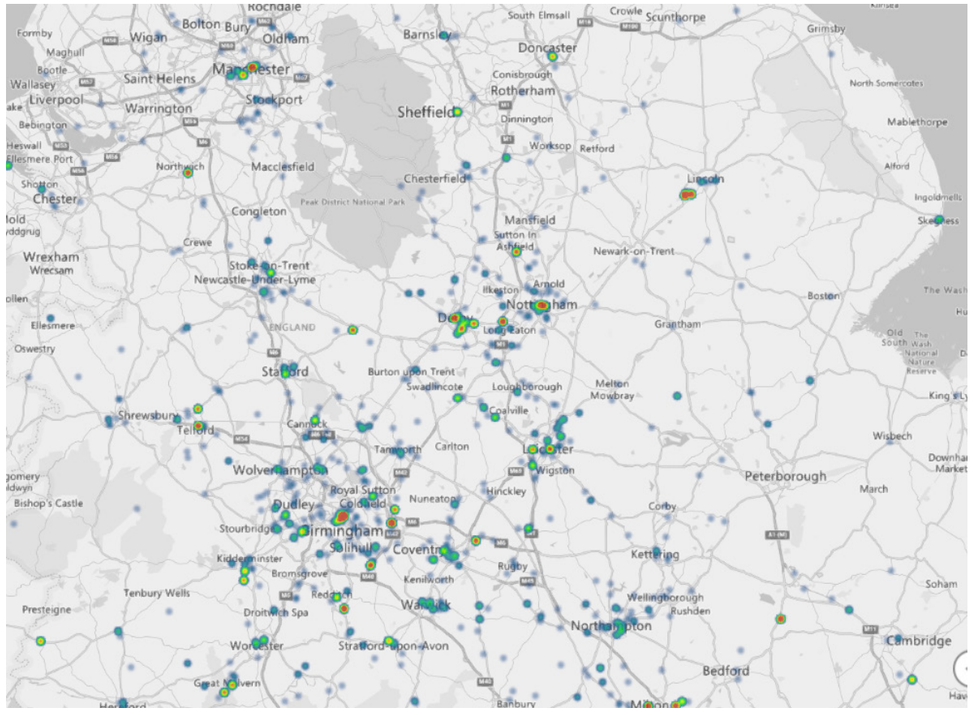
The region has attracted significant international investment (although largely through merger and acquisitions – demonstrating the global appeal), with more than 100 foreign-owned businesses in the area employing an estimated 19,000 people.

The Midlands benefits from five cyber and defence focused cluster networks —

- Midlands Cyber
- Three Counties Regional Defence & Security Cluster (TCRDSC)
- Greater Lincolnshire Regional Defence and Security Cluster (GLRDSC)
- West Midlands Cyber Working Group with further established networks in the East Midlands Cyber Security Cluster (EMCSC) and
- West Midlands Cyber Resilience Centre (WMCRC).

Further key industry networks engaging in this space include the Midlands Aerospace Alliance, Make UK Defence and Tech West Midlands. These organisations play a vital role in promoting and supporting cooperation and regional alignment between industry, the public sector and other stakeholders, enhancing the region's competitiveness both nationally and internationally.

2. This count includes businesses where a minority of their product/service feeds into the cyber & defence supply chain/applications but nonetheless play a role. Such businesses demonstrate resilience in the supply chain as they have diversified their market.
3. Cyber security sectoral analysis 2025 - GOV.UK



Data City Defence ISC (covering cyber and defence capabilities) – Midlands heatmap of business addresses in the Midlands – note concentration based on business count which includes registered and operating addresses. This map does not indicate employment concentrations, only business sites.

Midlands Cyber - supported by the UK Cyber Cluster Collaboration (UKC3) and based at Malvern Hills Science Park, Midlands Cyber is the official cyber cluster for the West Midlands, dedicated to supporting business growth, innovation, and digital security across key industries.

The cluster supports businesses to navigate cybersecurity challenges and develop new opportunities in sectors including:

- Defence & Security - Strengthening national security through advanced cyber resilience and threat intelligence.
- Manufacturing & Industry 4.0 - Protecting smart factories, supply chains, and automation from evolving cyber threats.
- Automotive & Mobility - Securing connected and autonomous vehicles, ensuring cybersecurity in transport innovation.
- Professional & Financial Services - Enhancing digital security, fraud prevention, and compliance for financial institutions.
- Digital Technologies & AI - Advancing cybersecurity solutions in cloud computing, AI, and data-driven innovation.

Midlands Cyber is headquartered in Cyber Valley, the heart of the West Midlands' cybersecurity ecosystem. Spanning Herefordshire, Worcestershire, and Malvern, Cyber Valley is home to the UK's largest concentration of cyber businesses outside London. With groundbreaking initiatives like the UK's first 5G testbeds, this cluster is a thriving hub for cybersecurity innovation, digital transformation, and cutting-edge technologies.

East Midlands Cyber Security Cluster – supported by UKC3 and based in Leicestershire, EMCSC was established in 2023 to facilitate collaboration, education and compliance guidance across the region's business community around cyber security.

Three Counties Regional Defence and Security Cluster (RDSC) – overlapping the Midlands Cyber cluster and covering Worcestershire, Herefordshire and Gloucestershire, 3CRDSC is one of the most established RDSCs in the UK, established to significantly raise the commercial and industrial capacity of the specialist defence & security technology and innovation sector. It also operates an annual defence trade show (Specialist Defence and Security Convention UK). Supported by the Defence and Security Accelerator, 3CRDSC connects SMEs with new contract opportunities and facilitates collaboration and innovation.

Greater Lincolnshire RDSC – covering Greater Lincolnshire and Turland, the GLRDSC is a network of defence and security businesses, working closely with the University of Lincoln. Lincolnshire is home to the RAF's Air and Space Warfare Centre, Air Battlespace Training Centre, and MOD Joint Cyber and Electromagnetic Activities group. With secure, large-scale military sites, extensive permitted air space, a low population density, and supportive communities, Greater Lincolnshire offers the ideal environment for defence businesses including: technology research and development, innovation, and testing and evaluation. The GLRDSC builds on the established ISTAR capabilities at RAF Waddington and within businesses supporting the RAF, combined with the University of Lincoln's leading-edge digital and information technology expertise, providing multiple collaboration and problem-solving opportunities.

West Midlands Cyber Working Group - part of the Innovation Alliance for the West Midlands, the Cyber Working Group connects cybersecurity experts, business leaders, and academics from across the West Midlands to promote collaboration and enhance cyber resilience. The CWG serves as a forum for sharing insights on emerging cyber threats, risk management, and cutting-edge security solutions. It is supported by Midlands Cyber and the WMCRC.

Despite the Midlands' established business community, several challenges hinder the industry's growth and investment. The available funding was reported by some participants to be underutilised by SMEs due to the perception that the defence sector is difficult to enter. Greater openness from government departments and bodies – to the extent possible without compromising security – is needed to avoid duplication of work and improve regional cohesion to the benefit of the national sector. While UK Research and Innovation (UKRI) collaborates with the Defence Science and Technology Laboratory (DSTL), a more joined-up approach is required across government bodies to reduce potential double-spending and streamline opportunities for dual use developments – such as the Department for Science, Innovation and Technology's Cyber ASAP programme, delivered by Innovate UK, which has funded £40m over 170 projects leading to 34 start-ups, but does not fund defence applications.

However, access to private equity and even bank finance remains a significant challenge for companies operating in the defence sector, or that could expand into it through dual use opportunities, as many UK banks and most other private equity firm's Environmental Social and Governance (ESG) frameworks and certifications such as BCorp hinder investment in defence-related activity. This relates to a wider societal perception noted in the UK that may perceive defence-related activity as unethical or unattractive, despite underpinning UK national security. Such sensitivities are exacerbated in the current geopolitical climate, as seen in protests noted at defence manufacturing companies.

Defence primes are uniquely positioned to direct funding through subcontracting and tenders. However some SMEs noted they have 'closed' supplier lists, making it challenging to secure a position in their supply chains. This demonstrates another opportunity for private finance to take a greater role in the market, supporting non-supplier SMEs and spinout opportunities during their critical early commercialisation. Given security controls around technology requirements such opportunities can be de-risked through collaboration with existing suppliers and the likes of the Defence and Security Accelerator (DASA).

However, there are dedicated accelerator funds such as through the NATO €1bn investment fund to support innovation (supported by DASA in the UK), SMEs and university-led research (Defence Innovation Accelerator for the North Atlantic – DIANA), with successes in the Midlands including Goldilock, selected for the DIANA accelerator programme to develop its unique physical network isolation solution "Drawbridge"[4].

The UK's digital economy faces an increasing threat from cyber-attacks, with critical sectors such as hospitals, universities, local authorities and government departments being targeted in recent incidents. High-profile attacks on the NHS and other national infrastructure highlight the severe consequences of cyber vulnerabilities. However, existing regulations have not kept pace with technological advancements, leaving gaps in cyber security and resilience. To protect national infrastructure, safeguard digital services and support economic growth, urgent action is needed to strengthen the UK's cyber-defences and implement robust regulatory measures- this needs to be done in concert with local industry through regional cyber clusters who can maintain oversight of developing technologies.

The Cyber Security and Resilience Bill, announced in the Kings' Speech (July 2024), aims to strengthen the UK's cyber-defences by closing regulatory gaps and enhancing the protection of critical services. It expands regulations to cover more digital services and supply chains, ensuring that emerging threats are effectively managed. Regulators will also gain stronger enforcement powers, including cost recovery mechanisms and the authority to conduct proactive investigations.

A key provision of the Bill is mandatory cyber incident reporting, particularly for ransomware attacks, to improve government awareness and response to cyber threats. This will enhance the UK's cyber-resilience, safeguard essential public services and support economic stability. However, industry is calling for firm regulations clearly defining cyber-security requirements. These standards must apply consistently to both security companies providing outsourced services and businesses managing their own defences to ensure a robust and uniform approach to cyber resilience.

A shift in perception is needed across lower tiers of manufacturing supply chains: cyber-resilience should be seen as a fundamental requirement rather than a revenue-generating function. Cyber-security protects people, businesses and critical assets, ensuring continuity and trust in an increasingly digital economy. Reframing cyber-resilience as a fundamental aspect of business protection – an essential cost of doing business – will help drive greater investment and prioritisation across all levels of industry.

Several participants commented on the underutilised capacity to address current cyber resilience issues across industry. Little infrastructure is needed to test many digital systems, and so demonstrators, resilience centres and tech companies themselves stand ready to engage their manufacturing (and other sector) peers to test and improve systems.

Doing this at scale, with support of the right entity such as Cyber Resilience Centres, Midlands Cyber or government, common issues can be identified and inform new regulations, while ensuring those businesses participating in such a programme are secure. This happens locally already in some initiatives such as the West Midlands Cyber Resilience Centre funding vulnerability assessments, however with poor uptake from SMEs, something that primes can help to address by encouraging their supply chains to engage.

4 NATO's Defence Accelerator (DIANA) Chooses Goldilock for Energy Resilience | Goldilock.com

Innovation

Although there is a buoyant active business population, one of the unique strengths of the Midlands in cyber and defence is its full ecosystem of innovation assets (research centres, technology parks and accelerators) through to end-users, with RAF Waddington among key national military assets (and end-users) in the region, along with proximity to GCHQ in Gloucestershire.

Considering these assets and major defence industry programmes such as at RBSL in Telford and Rolls Royce Submarines in Derby (AUKUS), there are 33 non-MOD innovation sites across the Midlands developing and supplying cyber security and related defence capabilities. Across these there are 59 distinct university research centres and defence training programmes specialising in topics from command operations to quantum technology. Nationally significant assets including the UK Telecoms Lab in Solihull to specialised business parks like Malvern Hills, Lincoln Science and Innovation Park, and MIRA Technology Park.

The higher standards for military use (particularly in hardware) are a key factor in the Midlands ecosystem – while established defence industry has the capability to meet these requirements, collaboration with innovators, universities and schools ensures a pipeline of talent and invention. Conversely, these standards can be challenging for new market entrants – and so engagement with demonstrators as well as accelerators, catapults and other industry support systems highlighted below are critical to successful commercialisation.

Existing defence platforms require significant cyber capabilities, as well as the integration of new cyber security technologies in older assets built 10 to 15 years ago. One example is modern naval propulsion systems, which rely on computer controls – and are thus dependent on their cyber security. This highlights a strong need to adopt a requirement to build in cyber models from the start, and legislation to ensure robust cyber resilience to identify and protect against emerging threats from fast-paced advancements in the ever more complex digital world.

Participants noted that a key challenge is the disparity between government contracts and private sector investment in research and development. While businesses are willing to commit significant private funding to innovation, the number of government contracts available does not match this level of potential investment – some argue the market is too small domestically, or 'closed' to new entrants. This gap risks slowing the commercialisation of new technologies and thus capabilities.

Key innovation assets and cluster sites include:

Malvern Hills Science Park (Worcestershire) – Situated in the heart of Cyber Valley, adjacent to QinetiQ and close to GCHQ, Malvern Hills Science Park (MHSP) is home to several growing companies working to strengthen the UK response to cyber attacks. The Park was established to facilitate the spin-out of companies eager to exploit QinetiQ's lead in technologies developed for military use but with potential commercial applications. MHSP provides excellent facilities to encourage the growth of high-tech companies, having high-quality accommodation and conference facilities in a beautiful situation nestling under the picturesque Malvern Hills.

Lincoln Science & Innovation Park (University of Lincoln)
Home to such businesses as Metrea Mission Data and SRC UK, LSIP has an established cyber and defence cluster particularly specialising in data and ISTAR, supported by the University of Lincoln and proximity to significant RAF presence including RAF Waddington, the home of UK ISTAR operations.

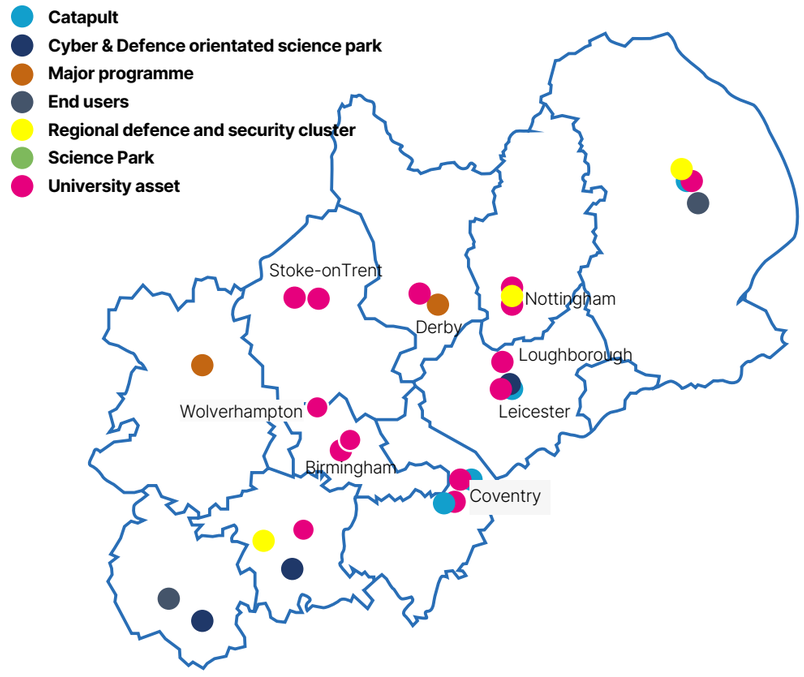
The University of Lincoln has established the **Centre for Defence and Security AI**, to support industry collaboration, including a memorandum of understanding with British defence technology company QinetiQ . It will focus on addressing the challenges in all areas of national security, including building security and resilience in multiple sectors, such as food and energy, and supporting effective strategic, operational and crisis decision-making in defence and beyond.

Skylon Park (Hereford) – Skylon Park has a strong focus on the Defence and Security sector, building on the deep-rooted association Hereford has with the UK special forces as the bases of the SAS. The park includes a Cyber Quarter for the Midlands Centre for Cyber Security. The existence of other key sites, DERA/QinetiQ in Malvern and GCHQ in Cheltenham, demonstrates a local cluster of strategic sites from which Skylon Park can draw. There is an inevitable emergence of businesses in the security sector. Herefordshire 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.

MIRA Technology Park (Warwickshire) – a world leading automotive engineering and innovation hub, with 40 major facilities UKAS accredited for defence standards and military specifications – with capabilities in vehicle engineering, test engineering and electronic defence.

Space Park (Leicester) – The University of Leicester's Spark Park is a hub for technology, innovation, science and knowledge-led industry. It's home to the National Space Centre and the highly successful Dock incubator, supporting innovative, knowledge-based technology businesses, including satellite and defence applications.

Manufacturing Technology Centre (Coventry) – while focused on manufacturing processes, the MTC is delivering a growing number of defence projects and is home to expertise on cyber security across manufacturing supply chains.



University-based research centres and relevant training initiatives include:

Aston University
- Aston Digital Futures Institute (ADFI).
- Aston Institute of Photonic Technologies.
- Cyber Security Innovation (CSI) Research Centre

University of Birmingham
- UK Quantum Technology Hub Sensors and Timing
- Centre for Cyber Security and Privacy

Birmingham City University
- Centre for Security and Extremism

Cyber Physical Systems (CPS) group

Cranfield University (although just outside of the Midlands, Cranfield is an active partner in the Midlands Innovation group of universities)
- Postgraduate academic provider to the UK's Ministry of Defence
- Cranfield Forensic Institute
- Advanced Materials for Protective Engineering Group: Blast and Ballistics
- Centre for Defence Chemistry
- Centre for Defence Engineering
- Centre for Defence Management and Leadership
- Centre for Electronic Warfare Information and Cyber
- Centre for Simulation and Analytics
- Counterterrorism, Intelligence, Risk and Resilience Group
- Ordnance Test and Evaluation Centre

Coventry University
- Centre for Trust, Peace and Social Relations, including 'Security, Vulnerability and Resilience'

De Montfort University
- Cyber Technology Institute

University of Derby
- Data Science Research Centre

Keele University
- Digital Society Institute
- Awarded Ministry of Defence Employer Recognition Scheme

University of Leicester
- Research Centre for Artificial Intelligence, Data Analytics, and Modelling

University of Lincoln
- Centre for Defence and Security AI
- Maritime Studies Centre, BRNC Dartmouth

- International Bomber Command Centre
- Intelligence, Surveillance, and Reconnaissance programmes
- Project Selborne (Royal Navy training programme)

Loughborough University
- Institute for Digital Technologies
- Centre for Security Studies
- TOXI-Triage
- Advanced VR Research Centre
- Collaboration with Defence Police Federation
- Darktrace PhD studentships

University of Nottingham
- Centre for the Study of Subversion, Unconventional Interventions and Terrorism
- Innovation, AI, Strategic and Defence and Procurement Research Unit
- National Cyber Security Centre certified degree
- CybSec

Nottingham Trent University
- Cyber Security Research Group
- Staffordshire University
- HM Forces courses
- Networks and Cyber Security (facilities)
- Centre for Smart Systems, AI, and Cybersecurity

University of Warwick
- Command, Leadership, and Urban Operations research
- Internet of Things Security Operational Test and Evaluation Centre
- International Technology Management for Defence and Security MSc
- International Relations and Security research cluster
- National Cyber Security Centre certified degree
- Cyber Security Research Network
- Secure Cyber Systems Research Group
- UK Advanced Propulsion Centre (APC)

University of Worcester
- Pro and Anti War Voices Conference
- Cyber Lab
- Living In Our Shoes

University of Wolverhampton
- Centre for Cyber Resilience and Artificial Intelligence
- Wolverhampton Cyber Research Institute
- Air, Space, and Cyber Power Studies
- Emergency Management and Resilience Centre

Catapults
- High Value Manufacturing Catapult (WMG, University of Warwick, HQ)
- Satellite Applications Catapult Centre for Excellence (University of Leicester)
- Energy Systems Catapult

Talent

Covering both cyber and traditional defence activities, the 600 Midlands-headquartered businesses employ an estimated 54,000 people nation-wide and generate more than £8.7bn in turnover annually.

The UK cyber security sector now employs an estimated 67,300 full-time professionals, reflecting a growth of around 6,600 roles over the past year—an 11% increase. The Midlands workforce consists of 13,000 cyber security professionals and more than 34,850 individuals working in defence and security, collectively contributing over £5 billion in GVA. The region accounts for 12% of the UK's total defence and security workforce, including 16,350 defence professionals and 18,500 in security roles. Salaries are competitive relative to other sectors, with UK Government's *Cyber Security Sectoral Analysis 2025* reporting a mean advertised salary of £55,700 in the East Midlands and £55,500 in the West Midlands. These salaries compete with most other regions except for Greater London & South East, the North East and Scotland.

There are a growing number of training pathways, from university programmes to apprenticeships, aimed at addressing the sector's evolving needs. Universities are actively working with schools to raise awareness of cyber careers, particularly among underrepresented groups, while institutions such as the Manufacturing Technology Centre and MIRA Technology Park are developing secure-by-design approaches that integrate cyber security with advanced engineering disciplines. Lincolnshire's RAF footprint (a significant location for force projection), Herefordshire and Shropshire's military presence further reinforce the Midlands as a strategic defence location.

Despite these strengths, challenges persist in building and retaining cyber talent. There are ongoing concerns about talent shortages, with businesses competing for a limited pool of skilled professionals. Many cyber-security and related degrees are heavily focused on software rather than engineering applications, leaving gaps in cross-disciplinary skills needed for cyber-resilience in engineering and manufacturing. Some business participants suggested that course content needs to be more influenced by industry requirements, which can be seen in practice at Loughborough University, which hosts PhD studentships with Darktrace – a global leader in cyber security AI.

Many apprenticeship schemes have seen success, but broader industry uptake is needed and some participants noted concerns about financial viability for some schemes and to partner universities and SMEs. Defence-specific careers face additional barriers, including lengthy security clearance processes that can deter potential candidates, and several businesses noted challenges in recruiting domestic graduates particularly with postgraduate qualifications – university participants noted a significant deficit in domestic masters and PhD students in relevant fields. The Midlands also struggles with graduate retention particularly in computing fields, where London salaries can be far higher.

There is growing recognition of the need to diversify entry routes into the sector. Universities are working with schools to promote cyber-security careers, important due to broad ignorance of the sector, particularly encouraging more diverse participation. Cyber First, run by the National Cyber Security Centre, is the government's programme to

encourage cyber security careers to young people, and has multiple school and further education partners in the West Midlands.

Industry leaders highlight the need for better-aligned training pathways, foundational computing and mathematical education, and clearer entry routes for mid and late-career professionals transitioning into cyber roles – an important route given the required skillset goes beyond software into areas such as decision making and risk management.

A significant challenge in the sector is the perception of cyber roles as too technical or inaccessible, with many potential recruits unaware of the breadth of careers available beyond coding.

Related, defence businesses *do* often have a distinct culture due to the sensitivities of their work and standards they adhere to, that compounded with perception challenges in parts of the population, create unique recruitment issues.

The Midlands' strong engineering and professional services workforce presents an opportunity for career changers, yet few structured transition programmes exist. Additionally, leadership at some organisations underestimates the importance of cyber resilience[5], leading to gaps in risk management and competent decision-making. Raising awareness of cyber-security as a critical enabler for all businesses , rather than a cost, will be key to strengthening the Midlands' position in cyber and defence innovation.

5. The Royal Navy notes that 97% of the world's data is transferred daily through undersea cables. If these were to all be inoperable, satellites could only pick up 3% of this demand load – a significant cyber resilience challenge with increasing threats to cables.

Growth and investment opportunities in the Midlands' cyber and defence industry

The Midlands can position itself as a national leader in cyber-security and defence innovation. With a thriving ecosystem of cyber firms, defence contractors and academic research centres, the region is primed to drive advancements in cyber-defence integration. The sector is rapidly growing, generating £12bn in turnover with 112 new cyber-focused firms established in 2024.

Nationally, the UK's cyber security industry has also seen impressive expansion. In the most recent financial year, the sector generated an estimated £13.2 billion in annual revenue, marking a 12% increase from the previous year (£11.9 billion)[6]. Cyber security-related gross value added (GVA) reached £7.8 billion - up £1.37 billion (+21%) compared to the previous year - reflecting the growing economic significance of the industry across the country.

As the UK faces rising cyber threats - 4 million attacks in 2024, of which 400,000 were successful- investment in cyber-resilience is more critical than ever. Within this national context, the Midlands stands out as a powerhouse of innovation and capability, ready to lead the charge in developing and deploying the technologies, talent, and partnerships needed to strengthen the UK's cyber defences.

Looking ahead, the following specific investment opportunities have been identified for businesses and financial institutions within the Midlands:

1. Complete supplier to end user 'ecosystem' with extensive business support capacity

As the home to several of the UK's most significant cyber defence programmes (UK Telecoms Lab, future armoured vehicles at RBSL Telford, AUKUS, RAF ISTAR operations from Lincolnshire and more), the Midlands is a significant market opportunity for suppliers in this space, as well as for identifying potential dual use opportunities across sectors.

This nascent opportunity is made more compelling by the extent of the local support system for cyber and defence applications, with internationally significant business and technology park activity – from sites such as the MTC and MIRA, to Malvern Hills and Lincoln, and regional demonstrators in 5G and more.

Focused training and research programmes ensure a pipeline of both talent and intellectual property with potential to commercialise.

With so much activity and primes to suppliers based in the region, the Midlands presents a competitive location for both business expansion and capital investment.

6 https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2025/cyber-security-sectoral-analysis-2025#fn:14

2. Specialisation over generic competition

With a complete cyber and defence ecosystem (innovators to end users all in the region), the Midlands has a unique opportunity to become a leading region in specific areas of cyber and defence, such as post-quantum encryption, connected and autonomous vehicles, supply chain resilience, digital manufacturing processes and 5G utilisation – both for domestic national security and as export opportunities. The region's vibrant innovation ecosystem has the capacity to generate many new spinouts and start-ups with the right investors engaging to develop these and dual use opportunities.

3. Securing the defence supply chain

Cyber vulnerabilities across supply chains (particularly tiers 2 and 3) threaten broader defence initiatives and the wider UK plc. The Midlands can lead in strengthening supply chain security by establishing robust standards, promoting best practices and supporting SMEs through funding and accreditation schemes. This is particularly important as the region leads in 5G technology adoption (the West Midlands being the first 5G demonstrator region, and home to the UK Telecoms Lab), increasingly digitalised manufacturing systems require cyber resilience.

4. Government support and defence innovation funding

The Defence and Security Accelerator (DASA) is a key partner in the €1bn DIANA fund to support innovation, SMEs and university-led research. A new 'defence innovation body' is soon to be announced[1] and MOD-backed innovation loans of up to £2m already provide critical financial support, with repayment required only once products become profitable. These funding initiatives present a major opportunity for Midlands businesses to scale operations, accelerate R&D and commercialise cutting-edge cyber-defence solutions. However, improving accessibility and awareness of these funds is essential to unlocking the full growth potential of the sector.

Additionally, the opportunity to collaborate with key allies such as Europe, the US and Australia continues to grow, particularly through trilateral programmes like AUKUS and anticipated access to the €150bn European rearmament fund. DASA plays a crucial role in facilitating these partnerships, with a future collaboration agreement expected to streamline direct opportunities for Midlands firms. With NATO's Innovation Accelerator set to launch, Midlands businesses must be well-positioned to leverage these international calls for innovation and investment.

5. Building a connected cyber and defence ecosystem including adjacent industries

This report highlights several cyber and defence clusters in the Midlands that are not necessarily connected, or when they are this collective value add is not recognised. Building stronger links between regional cyber hubs, industry and higher education institutions and presenting this ecosystem to businesses and investors with a single voice will encourage new investment, and could be an increased proactive role for cluster organisations such as Midlands Cyber or Combined Authorities through local growth plans. This increased connectivity should include established networks in adjacent sectors such as Aerospace, and relevant organisations such as the Midlands Aerospace Alliance and Tech West Midlands.

Government to turbocharge defence innovation - GOV.UK

6. Investor support

The Invest in UK University Research & Development Midlands campaign, promoting the collective capabilities of 20 universities in the region, profiles the Aerospace R&D facilities and expertise (including aspects of defence). The concierge service behind this campaign can connect businesses and funds looking to partner with researchers to commission research, development products and technology, commercialise IP and co-locate business activities in this thriving ecosystem.There are many investment promotion agencies and local initiatives such as Investment Zones and Freeports who can support prospective investors and businesses in navigating the Midlands and finding the right location to grow their business. A breakdown of these services is provided here.

Strategic asks

The Midlands already leads in cyber security and defence innovation, but targeted government action is essential to further unlock growth, investment and global competitiveness. To strengthen the sector and solidify the region's position, the following key strategic asks should be addressed:

1. Further professionalise cyber security to strengthen defence supply chains

The UK Cyber Security Council has established professional standards (i.e. to allow someone to be a Chartered Cyber Security professional[7], however there is a need to increase uptake. Businesses and academics have called for more bottom-up regulation and standards that keep pace with change, but ensure basic accountability across skills ***and*** products. With a full supplier to end user supply chain, and the demonstrators and business support in between, in the Midlands there is a unique opportunity to push this uptake and professionalise cyber capabilities.

Cyber vulnerabilities at Tier 2-3 supplier levels pose a significant risk to national security and industry resilience. Greater uptake of the National Cyber Security Centre's Cyber Essentials[8] programme will deliver highlighted need for SME support, although more is needed including funding for cyber audits, clear accreditation schemes and regulatory alignment, would raise cyber security standards across defence supply chains. This could have a positive secondary impact of creating local contract opportunities.

2. Secure long-term funding and clear policy

Sustained investment in cyber security innovation is critical. Government-backed funding, including grants for scaling businesses and tax incentives for cyber research and development, should be expanded. Additionally, clear regulatory frameworks must be established to ensure cyber-resilience is embedded in all defence projects (and beyond). The ecosystem should be more accessible with clear funding pots, support and stakeholders mapped out for an SME and investor audience, including explainers for engagement mechanisms like 'framework agreements' and more.

7. Become Professionally Registered
8. Cyber Essentials - NCSC.GOV.UK

3. Expand international collaboration and market access

With growing defence ties between the UK, US and Australia, and anticipated access to Europe's rearmament fund, there is a need to formalise agreements that enhance Midlands-based firms' participation in trilateral opportunities, including those under NATO's Innovation Accelerator. Support for Midlands firms in navigating international procurement and R&D partnerships will be key.

Domestically, greater collaboration is also needed between the national defence sector, armed forces, government departments, industry and academia. Streamlining these connections and funding pots will drive innovation, improve cyber-resilience and create a more cohesive approach to national security challenges.

4. Drive talent and workforce development

Flexible apprenticeship models at all levels (students to late career transfers), university-industry collaboration and dedicated funding for cyber skills training must be prioritised to address talent shortages. Expanding the Apprenticeship Levy to include the development of cyber-defence-specific industry- and university-led programmes and fast-tracking security clearance processes would help attract and retain talent.

5. Work to address cyber and defence industry profile *and* perceptions

Participants agreed on poor recognition of the breadth of career opportunities across cyber and defence businesses, and that this needs addressing from school careers advisors upwards – including stronger industry (particularly from SMEs with unique intellectual property) and university collaboration to confirm industry needs, particularly building on successful examples of postgraduate programmes for domestic students.

Beyond this, domestic defence and defence industry perceptions have changed over time. With initiatives such as BCorp and Environmental, Social and Governance frameworks driving investor decisions, as well as a diverse population with contrasting perspectives on the UK defence industry's impact internationally, defence and related business activity face unique challenges in availability of potential investors, as well as recruitment and even local public relations with some sites facing protests and other disruptions that hinder productivity.This issue is particularly pertinent on the investment front given predatory acquisitions of high growth businesses, particularly from US investors, seemingly not matched by UK capital availability.

This is part of a national conversation that government and industry itself must lead. Efforts should extend to recruitment pipelines, promoting defence-related job opportunities and career pathways, improving recognition in the public of the continued important of defence to their everyday lives. One example of this in practice is the Cyber First initiative[9]. While the school and college part of the programme is currently only available in the West Midlands and not the East Midlands, the wider provision is available to applicants from across the region – such as the UK Cyber Team competition[10].

9. CyberFirst Schools / Colleges - NCSC.GOV.UK
10. UK Cyber Team Competition

6. Connect and promote the Midlands as a cyber and defence innovation hub, developing regional market

Existing cyber cluster initiatives such as Midlands Cyber should be supported to play a wider specialist concierge service – connecting the myriad of assets highlighted in this report and particularly focusing on identifying dual use opportunities and demystifying the complex and secretive cyber and defence sectors for new market entrants and potential SME suppliers. This could include a coordinated campaign showcasing the region's capabilities, supported by trade missions and inward investment initiatives such as sectoral prioritisation in local growth plans and investment zones, would enhance visibility and global positioning.
This initiative begins at home – more can be done to stimulate a local market, with work to promote the importance of cyber resilience underpinned by showcasing ***where*** that resilience can come from, connecting local suppliers to potential clients.

By addressing these strategic asks, the Midlands can reinforce its leadership in cyber security and defence, driving economic growth while ensuring the UK's resilience against evolving cyber threats.

Conclusion

The Midlands cyber and defence clusters are a critical pillar of the UK's national security and technological advancement, with major industrial base and end-users based in or next to the region, and an extensive network of innovation hubs from university research to training programmes and industry-led technology demonstrators. With many of these assets arguably under-utilised, the region presents a unique opportunity for new businesses (and existing) to grow their operations and develop new products across cyber resilience, defence integration, and emerging security technologies.

However, to fully capitalise on these opportunities, a coordinated approach between government, industry and academia is essential. Increased support for SMEs to strengthen supply chain security, greater investment in cyber and defence innovation, and a clear regulatory framework able to keep pace with change and embed cyber-resilience across defence applications will be key to maintaining the region's competitive edge. Significant defence budget increases in the UK and European Union present a confirmed and growing market opportunity, particularly as these militaries pivot towards sovereign capability.

Talent development is a major priority, requiring better alignment between industry needs and skills provision. Expanding apprenticeships, addressing market accessibility and ensuring cyber security training integrates both software and engineering disciplines will be crucial in developing a sustainable workforce.

This report underscores the Midlands' role as a national leader in cyber and defence innovation. With the right strategic support, policy commitment and investment, the region will continue to strengthen the UK's cyber-resilience, attract global investors and drive the next generation of security and defence technologies.

Appendix

This discussion builds upon engagement with the following organisations:

Cyber & Defence Businesses

Alverium Associates
BAE Systems
Black Space Technology Limited
Blue Nebula Ltd
Cyber Chain Alliance
CyberCy
Cybur
Goldilock Secure Limited
Horiba MIRA Limited
IASME
In4 Group
Intelligent Storm Solutions Limited
Squidsoft ltd

Industry Bodies

EMCSC – East Midlands Cyber Security Cluster
Midlands Cyber
Horibra MIRA Limited
Manufacturing Technology Centre
Midlands Centre for Cyber Security
Warwick Manufacturing Group
WMCRC – The Cyber Resilience Centre for the West Midlands

Consultants & Data Providers

Arup
The Data City
Beauhurst
CBI Economics
Gowling WLG
Midlands Engine Observatory
Wavteq
Youp Consulting

Universities

Aston Centre for Cyber Security
Aston University
Cranfield University
De Montfort University
Loughborough University
University of Birmingham
University of Derby
University of Lincoln
University of Nottingham
University of Warwick
University of Wolverhampton

Growth Entities & Government

Defence and Security Accelerator
Department for Business and Trade
Department for Science, Innovation and Technology
Engineering and Physical Sciences Research Council
UKRI
Innovate UK
Invest in Coventry & Warwickshire
Invest in Leicester & Leicestershire
Royal Navy
West Midlands Combined Authority
West Midlands Growth Company