NW CYBERCOM

LOOKBOOK

Funded by UKRI Research England

Commissioned by Lancaster University

Delivered by plexal

In partnership with University of Salford Manchester, University of Liverpool, Manchester Metropolitan University, The University of Manchester, University of Lancashire

The £1.2m North West Cyber Security Connect for Commercialisation (NW CyberCom) project is a collaborative effort between the universities of Lancaster, Manchester, Salford, Liverpool, Manchester Metropolitan University and the University of Lancashire. Funded by Research England and supported by Plexal, it's unlocking the cyber security potential of the North West.

Funded by UKRI Research England

Commissioned by Lancaster University

Delivered by plexal

In partnership with University of Salford Manchester, University of Liverpool, Manchester Metropolitan University, The University of Manchester, University of Lancashire

We identified the most pressing cyber security challenges facing the North West and the UK, setting challenge statements to guide research and innovation. Academics responded with project proposals, receiving funding and mentorship from Innovators in Residence — experienced entrepreneurs who have successfully built and exited businesses.

Through this programme, researchers gained valuable insights into entrepreneurship, refining their ideas for commercialisation. They also engaged with industry leaders and potential buyers, ensuring their solutions address real-world cyber security needs.

Explore the projects, discover what our academics have learned and connect with us if you'd like to advise, invest, or collaborate with our future cyber founders.

Get in touch: nwcybercom@lancaster.ac.uk

The status and aims of these projects are accurate at the time of publication. For the latest updates and to connect with the teams, please contact nwcybercom@lancaster.ac.uk.

COHORT ONE

Our first set of projects tackled two critical cyber security questions:

1 | How can ethical AI enhance automated decision-making while reducing cognitive load in a cyber-secure way?

2 | How can AI or quantum technology ensure data authenticity and enable secure confidential data sharing?

USING AI TO PREDICT SOLAR FLARES AND PROTECT OUR TECH-DEPENDENT WORLD

Project lead

Professor Robert Walsh, University of Lancashire, supported by Dr Ndifreke Okon Nyah, Professor Silvia Dalla

Aim

Develop a real-time AI tool to forecast solar flares and their effects on Earth, enhancing our resilience to space weather.

The problem

Industries and agencies that depend on space and ground-based technologies face growing risks from solar flares, which can disrupt satellites, communication networks, and power grids. The lack of accurate, timely warnings leaves critical infrastructure vulnerable, with current systems struggling to predict events far enough in advance to take effective action.

Our solution

We're using AI to predict large solar flares—massive solar bursts that can disrupt communications, damage satellites, and cause power outages. With growing tech reliance, accurate forecasts are vital.

Developed with NASA colleagues, our AI uses over a decade of solar data to forecast flare timing and potential impacts at Earth's orbit.

Key insights & lessons learned

This project has underscored the importance of integrating AI with traditional scientific methods. A key lesson has been the importance of collaboration across disciplines – combining expertise in solar physics, AI and data processing has been crucial to our success.

I'd recommend focusing on scalability from the start. Our tool's ability to handle increasing data volumes has been essential and it's something to consider early in the development process.

ENHANCING MANUFACTURING SECURITY WITH AI-DRIVEN ANOMALY DETECTION

Project lead

Tarek Gaber, Senior Lecturer in Cyber Security, University of Salford, supported by Angel Jimenez-Aranda, Associate Professor in Digital Transformation, Salford Business School

Aim

Develop a secure AI model to detect and mitigate anomalies in manufacturing, improving efficiency and safeguarding against cyber threats.

The problem

In today's manufacturing industry, where digital and AI technologies are becoming essential, the risk of cyber threats has significantly increased.

Our solution

Our project develops an AI-driven anomaly detection model for manufacturing, like food packaging, to identify real-time irregularities and defend against AI threats such as model poisoning and evasion attacks. It aims to boost efficiency, minimize downtime, and enhance cybersecurity.

Key insights & lessons learned

We engaged industry stakeholders to validate our approach, receiving strong positive feedback—especially from those concerned about rising cyber threats in manufacturing.

NW CyberCom deepened our understanding of integrating AI and cybersecurity in manufacturing, highlighting the need for models that are both accurate and resilient to adversarial attacks. Collaboration between cyber experts and industry was key to addressing real-world challenges.

I recommend early, ongoing engagement with industry partners to ensure solutions meet practical needs and are deployable in real settings.

ENSEMBLE: AI-DRIVEN OSINT FOR ENHANCED INTELLIGENCE ANALYSIS

Project lead

Dr. Kyle Cunliffe, supported by Dr Christopher Murphy

Aim

Develop an AI-based tool, “Ensemble”, to enhance open-source intelligence (OSINT) by integrating intelligence analysis frameworks, improving accuracy and efficiency.

The problem

Whether governments, businesses or journalists, the goal is to streamline the analysis of vast, fragmented data, reducing human bias and enhancing decision-making. We aim to democratise intelligence tools, allowing even non-experts to benefit from advanced tradecraft.

Our solution

Ensemble is a pioneering software that combines AI and machine learning with intelligence analysis techniques to help organisations navigate complex, context-sensitive issues using OSINT.

Key insights & lessons learned

Ensemble has shown strong potential to reduce the time and cost of producing high-quality OSINT intelligence, delivering faster, more reliable insights. Early tests confirm its ability to automate complex analysis, enhance risk assessments, and support better decision-making. Feedback highlights its value in uncovering insights missed by human analysts.

Support from the NW CyberCom Connected Capability Fund has accelerated progress, enabling key collaborations with business partners, academics, and Salford University’s Innovator in Residence.

Development has underscored the value of collaboration between AI and intelligence experts, the need for iterative testing, and the importance of a simple, user-friendly interface. Future work will expand capabilities with multi-language support and more diverse analytical tools.

ENHANCING CRITICAL DATA HANDLING WITH AI AND QUANTUM TECH: FROM DEFENCE TO INDUSTRY

Project lead

Carl Nightingale at Manchester Metropolitan University, supported by Dr Tooska Dargahi

Aim

Leverage AI and quantum-inspired technologies to improve the speed and accuracy of handling sensitive and high-volume data in health and manufacturing sectors.

The problem

Current data-handling systems in sectors like healthcare and manufacturing are fragmented, manually intensive, and slow to adapt—leading to inefficiencies and potential errors.

Our solution

We’ve developed a platform that uses an advanced similarity detection algorithm—deployed either on-premises or in the cloud—to rapidly identify and match complex data patterns. Initially designed for military use, it has now been adapted to support critical operations in healthcare records management and smart manufacturing environments.

Key insights & lessons learned

Working with stakeholders across health and industry, we’ve shown how this technology can dramatically cut the time and effort required to process critical data securely and accurately. The pivot also demonstrated the versatility of AI and quantum-inspired algorithms across domains. Key insight: successful deployment depends on flexible architecture and close collaboration with users to ensure the solution fits real-world operational needs.

INNOVATIVE ROBOTICS FOR SAFER NUCLEAR SUBMARINE DECOMMISSIONING

Project lead

Dr. Mario Gianni, Senior Lecturer in Robotics and Autonomous Systems, supported by Babcock and University of Liverpool

Aim

Develop robots to safely inspect nuclear submarine pipes, reducing human exposure and saving costs.

The problem

Dr Mario Gianni explains: "*The decommissioning and disposal of nuclear systems is complex. Companies leading this process, face major challenges in assessing the residual radiation levels within the nuclear reactors' complex pipework, which makes it harder to classify the radioactivity levels and determine appropriate disposal routes. This is amplified as the systems are difficult for humans to access and too intricate for standard inspection tools.*"

Our solution

To tackle this, we're developing advanced robots that can safely navigate these pipes and monitor radiation levels without putting humans at risk. Our next steps involve enhancing the robots' security against cyber threats to make sure they operate safely and efficiently. This technology not only addresses a crucial industrial need but could also revolutionise the future of nuclear decommissioning.

Key insights & lessons learned

Our partnership with Babcock has been key to developing robots that safely inspect complex pipe systems, reducing radiation exposure and costs in the decommissioning process. Early integration of cyber security proved crucial for safe, reliable operation.

The project shows the power of interdisciplinary collaboration—combining robotics, nuclear engineering, and cyber security to create a practical, advanced solution. A key takeaway: prioritising security from the start saves time and resources later.

AI-DRIVEN CODE REPAIR: ENHANCING SOFTWARE SECURITY WITH ESBMC-AI

Project lead

Yiannis Charalambous, supported by Professor Lucas Cordeiro, The University of Manchester (Department of Computer Science)

Aim

Develop an AI-powered tool, ESBMC-AI, to automatically find and fix software vulnerabilities, improving security and freeing developers for creative tasks.

The problem

Large language models can generate code but often miss hidden security flaws.

Our solution

We're working on a tool called ESBMC-AI that uses advanced AI models and formal verification to automatically find and fix security vulnerabilities in software code. ESBMC-AI acts like a security expert, checking the code produced by the AI and making sure it's safe. If it finds an issue, it points out the problem and helps correct it.

Key insights & lessons learned

Collaboration with industry was key to shaping ESBMC-AI. Working with developers and cyber security experts helped guide its development, resulting in a tool that can automatically fix complex memory-related bugs—a major source of software vulnerabilities. Feedback has been positive, with clear value seen in its ability to detect and repair security issues.

The project shows the power of combining formal verification with AI, highlighting new opportunities in automated program repair. It also reinforces the value of interdisciplinary approaches and early industry collaboration in enhancing the relevance and impact of research

REVOLUTIONISING CYBER SECURITY WITH QUANTUM RING SINGLE-PHOTON LEDS

Project lead

Gizem Acar, supported by Professor Manus Hayne (Lancaster University)

Aim

Develop quantum ring single-photon LEDs to advance secure communications across various industries

The problem

As the demand for ultra-secure communication grows across sectors like telecoms, defence, and data centres, existing light sources fall short of the precision and reliability needed for quantum technologies. There's a critical need for scalable, high-performance, single-photon sources that can meet the security and speed requirements of next-generation networks.

Our solution

QR SPLEDs emit single photons at wavelengths used in today's fibre-optic networks, making them ideal for ultra-secure quantum key distribution. Unlike existing bulky, costly systems that require cooling, they're compact, low-cost, and work efficiently at room temperature.

Key insights & lessons learned

QR SPLEDs have attracted strong interest from finance and government sectors for enhancing data security without major infrastructure changes.

Collaboration with experts in quantum tech and cyber security was key to developing innovative solutions. Early and ongoing engagement with industry stakeholders helped align our research with real-world needs.

NW CyberCom played a vital role in advancing the project to proof-of-concept. Support from the Innovator in Residence boosted confidence in achieving product-market fit and commercial viability.

COHORT TWO

Our second set of projects tackled urgent cyber security concerns in manufacturing and healthcare, focusing on the following challenge statements:

1 | How can operational technology (OT) and the industrial internet of things (IIoT) be secured in manufacturing?

2 | How can healthcare organisations embrace digital transformation securely—minimising disruptions, protecting sensitive data, and improving resilience and recovery? Alternatively, how can internet-connected health devices be secured or designed with security at their core?

These projects explore innovative solutions to safeguard critical infrastructure, ensuring cyber security remains a priority in rapidly evolving industries.

SECURE EXOSKELETON TECHNOLOGY

Project lead

Matthew Dickinson, University of Lancashire, supported by Victoria Millsop, Graham Chapman and Giles Watkins

Aim

Build biometric security for exoskeleton technology within the industrial environment.

The problem

There's growing concern for cyber safety in wearable robotics, particularly manufacturing and military applications. Without the necessary security measures, exoskeletons may be hijacked or misused in ways that could compromise personal or operational safety.

Our solution

This project aims to revolutionise exoskeleton technology by integrating advanced cyber security measures to safeguard industrial and military applications.

We're implementing robust security protocols to ensure that only authorised users can operate the equipment, preventing unauthorised access, misuse, or cyber threats like malware. By embedding security at the core of the design, we enhance operational safety, reliability, and resilience.

Key insights & lessons learned

We used the funding to develop a proof of concept, including cyber security architecture design and testing with a view to delivering secure, high-performing exoskeletons that meet the demands of industrial, healthcare and military applications. We are exploring funding options for further development and commercialisation.

QUANTUM-SAFE SECURITY FOR LEGACY MEDICAL IOT DEVICES

Project lead

Safiullah Khan, Manchester Metropolitan University, supported by Mohammed Al-Khalidi, Yinka John Adegoke and Ryan Heartfield

Aim

Our aim is to enable secure, efficient and scalable data protection in healthcare systems.

The problem

There is an urgent need for secure, quantum-safe communication in legacy medical IoT (MIoT) devices, such as insulin pumps and pacemakers, that are used by clinical healthcare systems. These devices often lack robust encryption, which could put patients and vulnerable people reliant on these devices at risk.

Our solution

We have developed a solution that uses Ascon and ML-KEM, combining lightweight and quantum-safe cryptographic primitives. The solution has been demonstrated on a QEMU VExpress board and is being migrated to IoT devices and FPGA-based prototypes. It enables secure, low-power encryption for legacy MIoT devices, supporting integration with NHS systems and providing security support for medical device manufacturers, healthtech companies and healthcare providers.

Key insights & lessons learned

We've learned about how to effectively progress toward commercialisation. What stands out is the critical importance of engaging all project stakeholders – such as healthcare providers and industry partners – early in the process to ensure alignment with clinical needs and market expectations. In the future, we aim to license the technology so it can be used with legacy devices by the NHS.

SECURING OPEN WI-FI NETWORKS

Project lead

Dr Valerio Selis, University of Liverpool, supported by WiFiAlli Ltd and Paul Boardman

Aim

Validate a solution for public Wi-Fi networks to detect and prevent cyber attacks.

The problem

Public Wi-Fi hotspots put customers at risk of cyber attacks. One type of attack is the evil twin, where an attacker mimics the legitimate hotspot to deceive customers into connecting to it. Once they're connected, the attacker can intercept, monitor or manipulate their internet traffic.

Our solution

Our solution would enable the detection and prevention of cyber attacks while also providing analytics that enhance the security and performance of the monitored Wi-Fi hotspot. By operating independently from the existing infrastructure, it provides an additional security. It can be used in a variety of sectors, including healthcare and hospitality sectors.

Key insights & lessons learned

I've learned that successful innovation doesn't only rely on technological excellence, but also on how well a concept is communicated, as well as that moving fast is essential. Looking ahead, a patent will be filed for a newly created method to protect customers against a recently identified threat, for which additional funding will be required.

GENERATING PRIVACY-PRESERVING SYNTHETIC HEALTHCARE DATA

Project lead

Warren Del-Pinto and Viktor Schlegel, University of Manchester, supported by Yuping Wu, Goran Nenadic and Jeremy Goldstone

Aim

Develop an approach to enable safe and rapid innovation in healthcare research.

The problem

Due to the sensitive nature of clinical information, there's a lack of available data –particularly in free-text – to drive innovation in healthcare research. This creates difficulty specifying the computational and infrastructural needs of a given research project from the outset, creating delays in initiating research projects due to data access issues.

Our solution

By generating low-risk, high-quality, synthetic clinical free-text data, we can enable the development and deployment of proof-of-concept environments in the healthcare space, by making synthetic data available earlier in the research cycle. This will enable healthcare providers and external partners to collaborate more effectively, resulting in higher quality outputs and safeguarding of patient privacy.

Key insights & lessons learned

We've discovered potential models for commercialising our research, particularly which part of the research output should be commercialised – algorithm or data, for example. This includes key business considerations once we transition from pure research to deployment.

ENHANCING CYBER SECURITY IN QUANTUM COMMUNICATIONS

Project lead

Alessandro Romito, Lancaster University, supported by Dr Tara Kalsi and Jeremy Gidlow

Aim

To ensure quantum technology development has more secure and stable data and communications.

The problem

There is a growing need for secure quantum communication amongst data centres, and in the manufacturing and healthcare sectors. Quantum information and computation companies require the means to control and stabilise entanglement-generating dynamics for use in quantum sensing and quantum information processing.

Our solution

Based on newly created feedback mechanisms, we've developed an algorithm for high-fidelity cloning of quantum dynamics that generates redundancy in the states of interest, with seamless integration.

Key insights & lessons learned

Having conducted simulation testing, and explored a commercialisation strategy, the project now requires a commercial partner for delivery. I've learned about the process of choosing a suitable partner and negotiating a mutually beneficially agreement.

AI ASSISTANCE FOR HEALTHCARE

Project lead

Dr Tooska Dargahi, Dr Oluwaseun Ajao and Prof Mohammad Hammoudeh, Manchester Metropolitan University, supported by Mohammadreza Tabatabaei, Ifeanyi Bryan Uzoatu and Ryan Heartfield

Aim

The project has been designed to enhance security, privacy and compliance in the healthcare sector to make security governance information easily accessible for the end users.

The problem

There's a growing threat landscape where healthcare is the most targeted sector for cyber attacks, presenting significant cyber security and privacy challenges. Cyber incidents have reached their costliest point since 2011, valued at $9.77m in 2024.

Our solution

Our privacy-preserving AI assistant addresses challenges by providing immediate, context-specific guidance on security policies and compliance. It's designed to operate locally within healthcare organisations' infrastructure, eliminating third-party data exposure. Additionally, it implements robust defence against AI-specific attacks and simplifies complex security information for non-technical healthcare staff.

Key insights & lessons learned

While we haven't made changes yet, our focus is shifting towards industry needs to ensure real-world applicability and impact.

CRITICAL CYBER SECURITY GAPS IN IOT/OT DEVICES

Project lead

Zheng Xie, University of Lancashire, supported by Yvonne Kuma, Mohamed Zaid and Giles Watkins

Aim

Address cyber security vulnerabilities in IoT/OT devices.

The problem

Microcontrollers used in industrial and medical systems often lack robust protections due to limited processing power. There is a need to protect consumer and healthcare IoT devices from vulnerabilities in open Wi-Fi networks, such as Evil Twin attacks.

Our solution

The system we propose uses lightweight battery-powered portable devices to implement industry-standard data transfer security for biometric data. Starting with prototypes on Raspberry Pi platforms and transitioning to the Sonata microcontroller architecture, the initiative will culminate in a secure medical device for patient data collection, offering a scalable, practical solution for underserved markets. It doesn't require any user intervention or technical expertise.

Key insights & lessons learned

Following lab testing, field validation and data analysis, we are exploring commercialisation pathways.

About Research England
Research England is responsible for funding and engaging with English higher education providers, to create and sustain the conditions for a healthy and dynamic research and knowledge exchange system in the higher education sector.

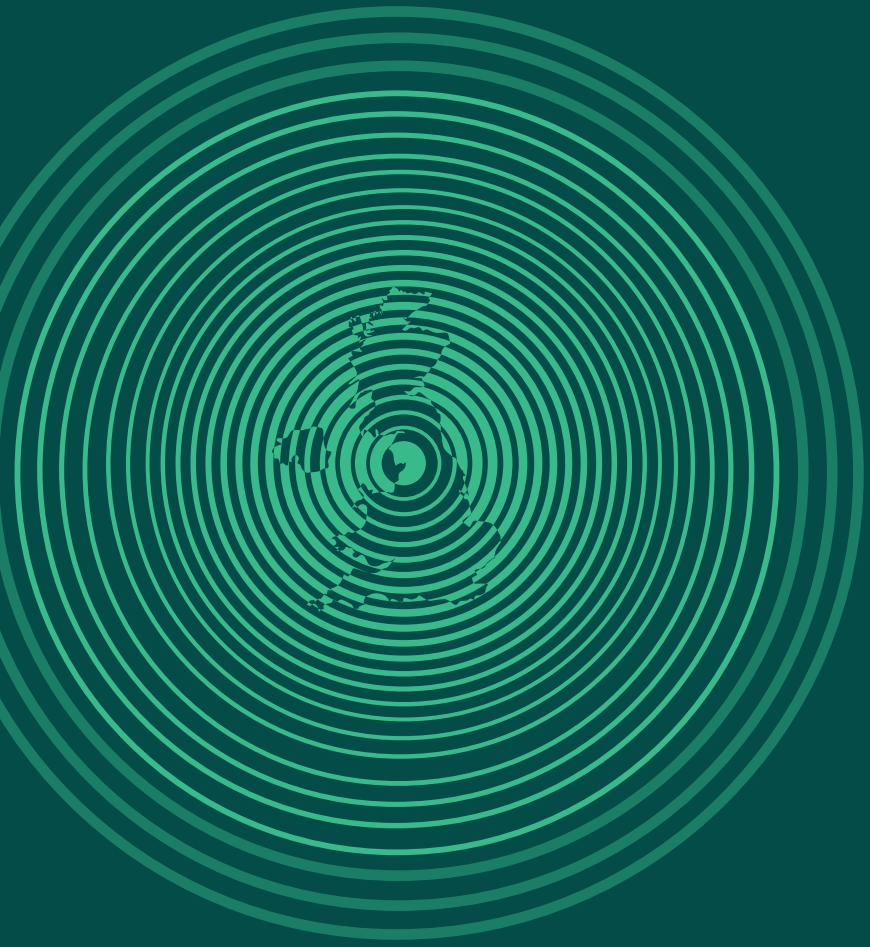
About Plexal
Plexal is committed to achieving the potential of emerging technology through strategic collaboration with the government, industry, startups and academia.

Founded by Delancey in 2017, Plexal works to solve society's most pressing problems through accelerating access to novel startup solutions by closing the gap between organisations – small and large, private and public, local and global. We're driving national security progress, economic growth and social prosperity by building physical places for innovation, delivering innovation services through programmes and consultancy and establishing regional clusters of excellence nationwide.

From offices in London, Manchester and Cheltenham, we've supported the growth of more than 1,200 businesses and contributed £731m to the UK economy since 2017, helping generate 9,400 jobs. And over the last 12 months alone, Plexal has unlocked £183m in gross value added, 25% of the total GVA from the last seven years, and helped create 2,360 jobs.

Of the companies supported by Plexal-run programmes, 141 have received funding and collectively raised £898m in investment and £69m in innovation grants.

Funded by UKRI Research England Commissioned by Lancaster University Delivered by plexal



Funded by UKRI Research England

Commissioned by Lancaster University

Delivered by plexal

In partnership with University of Salford Manchester, University of Liverpool, Manchester Metropolitan University, The University of Manchester, University of Lancashire