Cyber Security Academic Startup Accelerator Programme 21/22

Demo Day + 17 February 2022

Level 39 | Canary Wharf | London

+ Online

CYBER + ASAP

CyberASAP - Programme Context

The Department for Digital, Culture, Media and Sport (DCMS) is leading the government's work to develop the world's best and most secure digital economy. DCMS wants the UK to be the best place to start and grow a business.

The new National Cyber Strategy is the Government's plan to ensure that the UK remains confident, capable and resilient in this fast-moving digital world; and that the UK continues to adapt, innovate and invest in order to protect and promote our interests in cyberspace. This new strategy builds on the significant progress made through the National Cyber Security Strategy 2016-2021 and delivers on a commitment made in the government's Integrated Review of Security, Defence, Development and Foreign Policy which was published earlier.

Department for Digital, Culture Media & Sport

UKRI Innovate UK | ktn

The 5 Pillars

The Integrated Review set out five 'priority actions' which form the pillars of UK government's strategic framework, guiding and organising the specific actions we will take and the outcomes we intend to achieve by 2025:

Pillar 1

Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry

Pillar 2

Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected

Pillar 3

Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies

Pillar 4

Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power

Pillar 5

Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers

CyberASAP is funded by DCMS and delivered in partnership by Innovate UK (grant funding to universities) and Innovate UK KTN (programme delivery). In 2021 CyberASAP introduced a new funding stream for PETRAS projects, part of the Security of Digital Technology at the Periphery programme (SDTaP) funded by UKRI.

Expanding Skills

The only pre-seed accelerator programme in the UK's cyber ecosystem, CyberASAP helps convert great academic research into great cyber innovations. The programme provides a dynamic interface between government, cyber security academics and the business and investment communities that helps drive the growth and development of this key sector.

Led by a highly experienced team from Innovate UK KTN, with input and assessment from their expert industry connections, CyberASAP operates over three competitive stages:

PHASE 1

Developing a Value Proposition

Market Validation of the Value Proposition

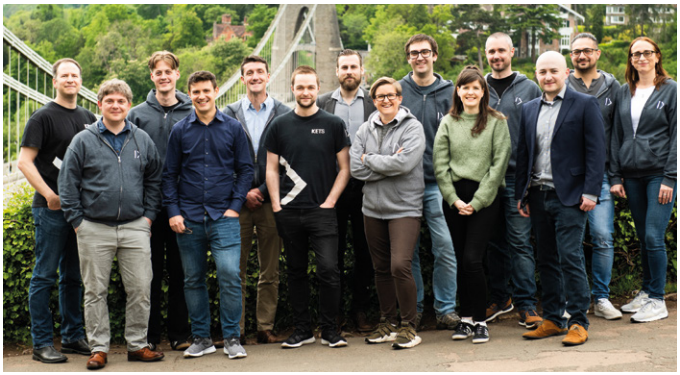
PHASE 2

Creating a Proof of Concept

Verifiable Credentials Ltd, CyberASAP Alumni, University of Kent

Driving Innovation

Commercial upskilling; an entrepreneurial mindset; exposure to new business concepts and language; advanced market research and comms techniques; insights into how investors think and work; honing effective presentation techniques - just some of the takeaways designed to give talented academics the confidence and know-how to translate their research into viable cyber products, technologies and services.

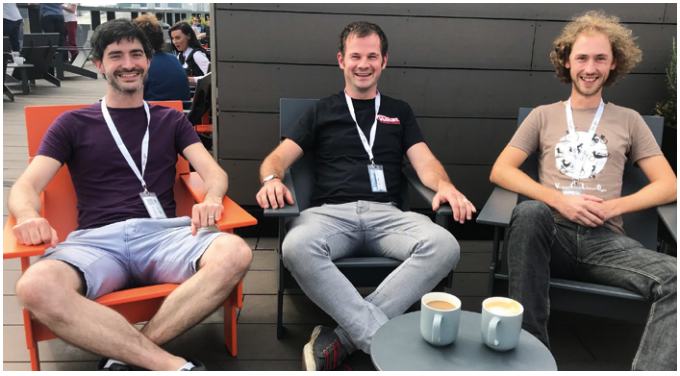


KETS Quantum Security, CyberASAP Alumni, Bristol University

Our Alumni have secured more than £17m in further funding to progress their projects. Successes come in many forms including: creating start ups (21 to date); acquisition by technology firms; receiving seed funding; joining other accelerator programmes; securing government grants; partnering with commercial enterprises. Read our **Impact Report** and **Case Studies** at **cyberasap.co.uk**

CAPSLOCK, CyberASAP Alumni, University of Bradford

There's no single pathway for the talented academics who participate in CyberASAP. But what unites them is the value they draw from being on the programme: the knowledge gained can enrich their ongoing work either within academia or industry, creating more opportunities to extend the impact of their experience.



Graphics Fuzz, CyberASAP Alumni, Imperial College London

Event Running Order

Agenda

Welcome:

Dr Emma Fadlon, Co Director, CyberASAP, Innovate UK KTN

Keynote:

Julia Lopez MP, Minister of State for Media, Data, and Digital Infrastructure

Pitches from CyberASAP Teams:

From the final 10 teams from CyberASAP 2021/22
(See running order for Team pitches on next page)

Tabletop Showcase/Demonstrations, Networking and Drinks:

Meet the teams and see their Proofs of Concept
(Videos of all teams' Demonstrators will be available at cyberasap.co.uk)

THANK YOU TO ALL OUR MENTORS & COLLABORATORS

CyberASAP is a collaborative enterprise, drawing on the experience and knowledge of Innovate UK KTN's Programme Directors, Emma Fadlon and Robin Kennedy, and their expert connections. This extended network of industry specialists who generously lend their expertise and insight to the academic teams is central to the success and impact of CyberASAP. *A huge thank you to each and every one of you.*

Team Pitches Running Order

Our interactive menu can be clicked on:

CYBER + ASAP

The Teams

UltraNetAI

UltraNetAi

Network search technology for front-line policing


Prof. Martin Reed


Prof. Klaus McDonald Maier


Dr. Xiaojun Zhai


Philip Cheung


Michal Borowski

Police forces in the UK need to deal with over 10,000 online sexual crimes against children and vulnerable adults each year. However, front-line officers lack the technology they need to perform searches for the devices that perpetrators are using to commit these crimes.

UltraNetAI will enable thousands of police officers to protect society against these serious offences. Our innovation embeds novel machine learning expertise from the University of Essex into a small unit for police entering a crime scene to gain essential forensic information about networked devices at a property. UltraNetAI is a simple plug-and-play solution that simply requires front-line officers to connect our device to home routers and then receive the intelligence they need directly to their mobile phones in real-time. Unlike competitors, we uniquely support UK police workflows for front line officers that do not have full forensic or technical training. Through encrypted cloud storage and connectivity, our solution allows forensic teams to audit the search, ensuring evidence is appropriately secured to enable convictions. Future UltraNetAI products will enable protection for children and young adults in education.

Contact Us

ultranetai.com

info@ultranetai.com

/company/ultranetai

Cyber Type

- Incident response and management
- Threat intel, monitoring, detection and analysis

Target Market

- Law enforcement

University of Essex

CyberSignature

CyberSignature delivers secure and frictionless online checkout authentication with digital behaviour intelligence.


Dr. Nonso Nnamoko


Prof. Yannis Korkonzelos


Joseph Barrowclough


Michael Boyle

Cyber criminals can easily steal our credit card numbers and personal details. This, combined with the dramatic increase in online transactions, makes protecting our personal details whilst shopping online that much more important.

CyberSignature adds an extra layer of online payment authentication that leverages unique user characteristics that are impossible to steal, such as typing speed, cursor movement habits and preferences to use the mouse, touchpad, or trackball. Capturing and modelling such parameters with Machine Learning creates a unique profile for the legitimate card owner. This is then used to distinguish them from cyber-criminals while carrying out a transaction online.

Contact Us

cybersignature.co.uk

nnamokon@edgehill.ac.uk

@cybersignature

Cyber Type

- Identification, authentication and access control

Target Market

- Financial Services

Edge Hill University

RIBB

SAFETY & SECURITY THROUGH DISTRIBUTED LEARNING

Royal-Imperial Black Box (RIBB)

Moving Target Defence for Enhanced Protection of Cyber-Physical Systems

Prof. Keith Mayes

Dr. Fei Teng

Dr. Martin Higgins

A collaboration between the Control and Power Group at Imperial College and the Royal Holloway cyber-security team. The RIBB offers enhanced cyber-physical security for utility systems to ensure bottom-up protection against deception attacks on utility network SCADA systems.

The RIBB is a post-intrusion defence solution providing both detection and recovery from sophisticated deception style cyber-attacks. The RIBB combines sophisticated distributed monitoring analytics with Moving Target Defences to enhance utilities networks against motivated attackers seeking to commit false data injection or replay attacks.

Contact Us

martin.higgins11@imperial.ac.uk

Cyber Type

- SCADA and info control system
- Threat intel, monitoring, detection and analysis

Target Market

- Government
- Energy / Infrastructure

Imperial College London

ROYAL HOLLOWAY UNIVERSITY OF LONDON

FeDCam Limited

Ground-breaking new federation of AI-based cameras to transform crime detection & policing

Prof. Mohammad Pat-wary

Difficulty in identifying a suspect is one of the main barriers to crime policing; it also encourages repeat offenders; and costs different sectors of our economy billions of pounds each year. For example the retail sector reported 79% repeat offenders, costing £4.88bn in 2019.The scale of the problem is consistent in most of the OECD countries. Surveillance technology spending in the UK is £2.2bn each year, where the associated software intelligence market is 10-15% of the overall spending.

FedCam is an innovative software solution & third party platform that creates a secured federation of surveillance cameras which fully automates end-to-end surveillance systems, from event prediction and detection to GDPR compliant evidence provision for successful prosecution. Our AI based solution uses multi-biometric data for offender identification, which significantly reduces false alarms compared with existing solutions. Our one-stop evidence shop approach enhances productivity in crime policing, reduces time for offender prosecution, discourages offenders from getting involved and saves money for the end-user (subscription cost will be low because of minimal IT requirement at the local level, which also reduces the cyber threat).

Contact Us

fedcam.co.uk

info@fedcam.ac.uk

Cyber Type

- Incident response and management
- Cyber-Physical

Target Market

- Energy / Infrastructure
- Automotive / Transport
- Healthcare
- Retail

OSIRT
Investigations, simplified

OSIRT

Online Investigations, Simplified


Dr. Joseph Williams


Jeeta Aulak


Dr. Stilianos Vidalis

80% of peacetime intelligence is obtained from open sources, so open source collection is a crucial tool for the modern cyber investigator.

OSIRT is your investigation, simplified; it provides a comprehensive, all-in-one platform from artefact capture to report to court, all without the need to be an expert user. OSIRT is cross-platform and plugs into your browser, ensuring the full and transparent capture of online artefacts, such as screenshots, source code and embedded videos.

OSIRT builds your case in the background, maintaining a chronological list of your activity so you can just focus on your online investigation. OSIRT has built a strong user base since its invention in 2015, from law enforcement to private investigators, with over 50,000 downloads to date from users across the globe.

Contact Us

osirtbrowser.com
j.williams30@herts.ac.uk
@OSIRTBrowser

Cyber Type

- Professional Cyber services
- Threat intel, monitoring, detection and analysis
- Digital and online investigations

Target Market

- Government
- Financial Services
- Law Enforcement

University of Hertfordshire UH

WalletFind

WalletFind

Discover it, Recover it, Control it, WalletFind manages your cryptocurrency wallets and activities


Dr. Sana Belguith


Dr. Tooska Dargahi


Prof. Mohammad Hammoudeh

The global size of the cryptocurrency market is expected to reach around $5T by 2030. Cryptocurrency has gone mainstream amid an increase in demand from financial institutions, investors, businesses and untapped potential applications. In 2020, 13% of criminals used cryptocurrencies for money laundering and an estimated $140B cryptocurrency has been lost due to forgotten passwords, file corruption or deletion.

WalletFind allows cryptocurrency investors, law enforcement and financial auditors to perform automatic deep cryptocurrency forensics to recover forgotten passwords and restore corrupted or deleted data from software and hardware-based wallets. It has the capability of conducting e-discovery forensics to track, trace and monitor illicit transactions and mining activities, and perform standard auditing tasks.

Contact Us

sana.belguith@bristol.ac.uk

Cyber Type

- Professional Cyber services
- Threat intel, monitoring, detection and analysis

Target Market

- Government
- Financial Services
- Energy / Infrastructure
- Automotive / Transport
- Healthcare
- Retail
- Manufacturing

University of BRISTOL

University of Salford MANCHESTER

Manchester Metropolitan University

MLighter

The holistic tool for security evaluations of machine learning systems

Dr. Héctor
D. Menéndez

Dr. Madhi Aiash

Machine learning (ML) fuels industry 4.0 and is increasingly becoming a cornerstone to support smart systems. ML allows us to learn from data and to provide a timely and accurate response to specific intelligent requirements. Despite their undeniable advantages, ML has not been deployed to its full potential. One of the main concerns during the deployment of ML-based systems is the fact that the ML models might be vulnerable to potential blind-spots in the forms of security vulnerabilities, performance issues, or unknown responses. While being system-dependent, our research found out that existing software testing tools and techniques can hardly be applied to identify these ML blind-spots because these tools do not take into account details such as correctness, optimal learning rates, over-fitting, feature computation, gradient computation, and optimal regularization, among others.

MLighter is the first tool to integrate and simplify multiple testing strategies to detect blind-spots in machine learning. It verifies the performance, security and functionality of your ML system, ahead of cyber-attacks. Our clients are coders and QA Testers of ML systems who need to evaluate the quality of their final ML products. This requires knowledge in different aspects of the developed systems and the used ML libraries. Our web-based solution includes the tools our clients need for the automatic validation of ML systems in terms of performance, security and functionality. It includes a database of blind-spots and vulnerabilities and a flexible front-end designed to allow extensions.

Contact Us

mlighter.freedevelop.org
mlighter@freedevelop.org
@HectorDMenendez
/in/hector-d-menendez

Cyber Type

- Professional Cyber services

Target Market

- Government
- Financial Services
- Automotive / Transport
- Healthcare
- Retail

Middlesex University London

TYMLO TECHNOLOGY

Tymlo Technology Ltd

An innovative platform consisting of three toolkits ensuring trust, quality and explainability to AI-based decisions

Dr. Ali Sadiq

Dr. Hiran Patel

Prof. Prashant Pillai

This project has developed a secure and trustworthy AI platform suitable for AI developers and data scientists, which provides a scoring mechanism to measure the quality and trust levels of datasets and AI/ML algorithm during development and deployment phases. The TrustMe platform is running based on a local-host web application with enabled features for designing, developing, and implementing explainable and trustworthy AI applications. TrustMe platform also offers a data quality score using Quality of Data (QoD) estimator.

Using QoD feature, end users can obtain the quality level of their data along with auto generated reports highlighting all bad records. QoD also offers an automated solution to enrich quality of data or perform data processing according to pre-defined and editable rules by data admins. To deal with possible bias within training/testing data samples, TrustMe offers Quality of Training/Testing (QoT) toolkits. This tool will help developers to automatically generate training/testing samples with considering over/below sampling for imbalanced data samples due to data acquisition process.

We envisage that in the next three years TrustMe Score and generated reports would become like a universal score that all organisations would want to use to prove how secure and trustworthy their AI platforms are.

Contact Us

tymlo.co.uk

info@tymlo.co.uk

/company/tymlo

Cyber Type

- Professional Cyber services
- Secure and Trustworthy AI

Target Market

- Government
- Financial Services
- Automotive / Transport
- Retail

UNIVERSITY OF WOLVERHAMPTON
KNOWLEDGE • INNOVATION • ENTERPRISE

Tensorcrypt

Empowering organisations to securely share and analyse confidential datasets

Dr. Carlton Shepherd

Prof. Konstantinos Markantonakis

Sharing data with key partners has never been more important for data-driven organisations. Yet, achieving this securely and efficiently remains an unsolved problem. Traditional solutions expose data at some point in the processing chain, whether when it is used, stored, sent, or received. In recent years, these issues have been at the foundation of several highly publicised data breaches.

To address this, Tensorcrypt is an innovative data sharing platform that provides data scientists, analysts, and engineers with a sandboxed environment for sharing and analysing sensitive information with internal and external users. The solution addresses in-transit, at-rest, and in-use information exposure risks, and is designed for high-throughput and low-latency applications. Tensorcrypt offers trackable data interactions for management and audit stakeholders, as well as simple API-level access to end users.

Contact Us

tensor.software

carlton.shepherd@rhul.ac.uk

/company/tensorcrypt

Cyber Type

- Secure data sharing

Target Market

- Government
- Financial Services
- Pharmaceuticals

ROYAL HOLLOWAY UNIVERSITY OF LONDON

taimas

TAIMAS

Building Management System (BMS) cyber-attack and tamper detection in a single box 'system as a service' solution

Prof. Jeremy Watson

Dr. Nilufer Tuptuk

Tony Williams

TAIMAS (Timing Anomalies as an Indicator of Mal-intervention in Automation Systems) is a single box solution to detect cyber-attacks and physical tampering against building management systems and industrial control systems. It is aimed at clients dissatisfied with high-cost enterprise-derived security approaches that mainly do network traffic monitoring and network attack detection. TAIMAS offers a new method independent of network traffic. Air-gapped monitoring of control system hardware utilising machine learning and both hardwired and cloud based threat notification

Our target market is the currently poorly protected population of legacy and newly installed building management systems in critical national infrastructure services, government, retail and hospitality. Users and operators of buildings in these sectors have immediate concerns about the adequacy of current cyber-protection measures available for their building management systems. TAIMAS will provide a cost-effective solution with a low impact, installation independent approach that ensures clients get early warning of any suspicious activity including Zero-day attacks. TAIMAS will include a range of additional optional functionalities including predictive maintenance.

Contact Us

jeremy.watson@ucl.ac.uk
/jeremy-watson

n.tuptuk@ucl.ac.uk
/nilufer-tuptuk

tony.williams@cubecontrols.co.uk
/tony-williams

Cyber Type

- Network Security
- SCADA and information control system
- Threat intel, monitoring, detection and analysis

Target Market

- Government
- Energy / Infrastructure
- Healthcare
- Retail
- Manufacturing

UCL

Get involved in CyberASAP

Academics

CyberASAP welcomes participation from academics based all around the UK who have an interest in commercialising their cyber research. The programme is particularly keen to invite applications from academics in under-represented groups.

For 2022/23 there are two funding streams:

- **Open Competition: applicable to any UK-based academic**
- **SDTaP Competition: open to PETRAS projects participating in the Security of Digital Technology at the Periphery (SDTaP) programme, funded by UK Research and Innovation (UKRI).**

The funding competition for the 2022/23 programme is open between **7 Feb 2022 and 2 March 2022.**

More information at **cyberasap.co.uk**

Mentors

Investors and industry colleagues with an interest in supporting the programme in any way are invited to provide their details at cyberasap.co.uk. We're always looking to extend our network of independent experts who provide such valuable input to the teams and enjoy insights into the cyber innovations being developed on the programme.

"CyberASAP is a brilliant initiative for early-stage academic cyber security startups, giving their ideas commercial rigour to form go-to-market strategies in order to create fully functioning and attractive businesses solving serious problems. We at Mercia have been supporting the programme for many years now and have seen the great work CyberASAP has achieved through the high-quality companies coming through from start to finish."

Jake Christoforou, Mercia Asset Management

Cyber Security Academic Startup Accelerator Programme 21/22

Year 5 Demo Day ✢ 17 February 2022

Level 39 | Canary Wharf | London ✢ Online

CyberASAP Programme Directors

Robin Kennedy
Cyber Security
robin.kennedy@ktn-uk.org
+44 7870 899956

Dr Emma Fadlon
Investment
emma.fadlon@ktn-uk.org
+44 7964 551643

CYBER ✢ ASAP
cyberasap.co.uk
@CyberASAP
cyberasap@ktn-uk.org
/cyberasap

UKRI Innovate UK | ktn
ktn-uk.org
@KTNUK