AMLUCS

APPLIED MACHINE LEARNING FOR CYBER SECURITY

Technical Conference

9th & 10th September 2025
We The Curious, Bristol

Conference Agenda

Brought to you by

FRAZER-NASH
CONSULTANCY
A KBR COMPANY

Sponsored by

AWERIAN

In partnership with

[dstl]
Delivering
Mission Success

CyBOK

CRANE
Cyber Security Research Network

women
in cyber

Day One – Tuesday 9th September

Next steps for Autonomous Cyber Defence

09:30 - 10:00	**Registration & Refreshments**
10:00 - 10:15	**Welcome & Introduction to AMLUCS** *Alex Revell, Frazer-Nash Consultancy*
10:15 - 10:45	**Keynote: Vulnerability of AI and Resulting Risk** *Sadie Creese, Professor of Cyber Security, University of Oxford; Founding Director, Global Cyber Security Capacity Centre; Strategic Advisory Board Member, World Economic Forum.*
10:45 - 11:15	**Adaptive by Design: Contextual Reinforcement Learning for Mission-Ready Cyber Defence** *Jake Thomas, Advai*
11:15 - 12:00	**Break & Refreshments**
12:00 - 12:30	**Autonomous Cyber Resilience: An Infrastructure-as-Code Approach for Coalition Military Networks** *Dr Konrad Wrona, NATO Communications and Information Agency*
12:30 - 13:00	**Deploying Autonomous Cyber Defence onto a Military Relevant Physical System** *Alec Wilson, BMT*
13:00 - 14:15	**Lunch & Poster Viewings** *(The Annexe)*
14:15 - 15:00	**Panel: Operationalising AI - Integrating Machine Learning into Defence Cybersecurity Systems** *Helen Wilson, Dstl, with Ministry of Defence stakeholders.*
15:00 - 15:15	**Autonomous Defensive Cyber** *Wayne Gould & Lara Tolley, Dstl*
15:15 - 15:45	**Break & Refreshments**
15:45 - 16:15	**Simulation-to-Reality Gap via RL-trained ROSbots** *Dr Jack Smith, Awerian*
16:15 - 16:45	**Topological Extensions for Reinforcement Learning Agents (TERLA).** *Tim Dudman, Riskaware*
16:45 - 17:00	**Day One: Closing Remarks** *Alex Revell, Frazer-Nash Consultancy*
17:00 - 19:00	**Drinks Reception** *(Exhibition Space)*

Day Two – Wednesday 10th September

Red Agents, AI Security & Evaluations

09:00 - 09:30	**Morning Refreshments**
09:30 - 09:45	**Day Two: Opening Remarks** *Alex Revell, Frazer-Nash Consultancy*
09:45 - 10:30	**Keynotes: Including the impact of AI on cyber threat from now to 2027** *Peter H & Annabel W, NCSC*
10:30 - 11:00	**RAGING MINOTAUR: Improving Defence against AI-driven Cyber-Attacks by Designing More Capable Autonomous Cyber Training Adversaries** *Althea Waites & Sharaz Anwer, Dstl*
11:15 - 11:30	**Lessons Learned in the Application of Reinforcement Learning Agents for APT Attack Path Generation** *Chad Caison, Six24 Cyber Labs, SIEGE team, DARPA CASTLE*
11:30 - 12:00	**Break & Refreshments**
12:00 - 12:30	**Defending Large Language Models against data poisoning** *Dr James Titchener*
12:30 - 13:00	**Text2VLM: Adapting Text-Only Datasets to Evaluate Alignment Training in Visual Language Models** *Gabriel Downer, Advai*
13:00 - 14:00	**Lunch & Poster Viewings** *(The Annexe)*
14:00 - 14:30	**A Statistical Pipeline for Uncertainty Quantification in ACD Test and Evaluation** *Dr Miriam Apsley & Dr Alessio Zakaria, Smith Institute*
14:30 - 15:00	**Modelling adversarial behaviour to enable AI predictions analogous to counterfactual reasoning** *Dr Louis Gauntlett, Frazer-Nash Consultancy*
15:00 - 15:15	**Closing Remarks** *Alex Revell, Frazer-Nash Consultancy*