



# AMLUCS

APPLIED MACHINE LEARNING  
FOR CYBER SECURITY

## Technical Conference

---

9<sup>th</sup> & 10<sup>th</sup> September 2025  
We The Curious, Bristol

---

# Conference Agenda

Brought to you by



Sponsored by



In partnership with



# Day One - Tuesday 9<sup>th</sup> September

## Next steps for Autonomous Cyber Defence

09:30 - 10:00	<b>Registration &amp; Refreshments</b>
10:00 - 10:15	<b>Welcome &amp; Introduction to AMLUCS</b> <i>Alex Revell, Frazer-Nash Consultancy</i>
10:15 - 10:45	<b>Keynote: The Human-AI Cyber Security Paradox</b> <i>Emma Arakas, Principle Consultancy, Frazer-Nash Consultancy</i>
10:45 - 11:15	<b>Adaptive by Design: Contextual Reinforcement Learning for Mission-Ready Cyber Defence</b> <i>Jake Thomas, Advai</i>
11:15 - 12:00	<b>Break &amp; Refreshments</b>
12:00 - 12:30	<b>Autonomous Cyber Resilience: An Infrastructure-as-Code Approach for Coalition Military Networks</b> <i>Dr Konrad Wrona, NATO Communications and Information Agency</i>
12:30 - 13:00	<b>Deploying Autonomous Cyber Defence onto a Military Relevant Physical System</b> <i>Alec Wilson, BMT</i>
13:00 - 14:15	<b>Lunch &amp; Poster Viewings</b> ( <i>The Annexe</i> )
14:15 - 15:00	<b>Panel: Operationalising AI - Integrating Machine Learning into Defence Cybersecurity Systems</b> <i>Helen, Dstl, with Ministry of Defence stakeholders.</i>
15:00 - 15:15	<b>Autonomous Defensive Cyber</b> <i>Wayne &amp; Lara, Dstl</i>
15:15 - 15:45	<b>Break &amp; Refreshments</b>
15:45 - 16:15	<b>Simulation-to-Reality Gap via RL-trained ROSbots</b> <i>Dr Jack Smith, Awerian</i>
16:15 - 16:45	<b>Topological Extensions for Reinforcement Learning Agents (TERLA).</b> <i>Tim Dudman, Riskaware</i>
16:45 - 17:00	<b>Day One: Closing Remarks</b> <i>Alex Revell, Frazer-Nash Consultancy</i>
17:00 - 19:00	<b>Drinks Reception</b> <i>(Exhibition Space) and MU</i>

# Day Two - Wednesday 10<sup>th</sup> September

## Red Agents, AI Security & Evaluations

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