AMLUCS

APPLIED MACHINE LEARNING FOR CYBER SECURITY

Technical Conference

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

CALL FOR SUBMISSIONS

Brought to you by

FRAZER-NASH CONSULTANCY
A KBR COMPANY

In partnership with

[dstl]
Delivering Mission Success

AMLUCS 2025 Call for Submissions

Unlock the future of cyber security at Applied Machine Learning for Cyber Security (AMLUCS) 2025.

Join Cybersecurity and AI/ML experts, industry representatives, and academic researchers as they present the latest advancements in the intersection of cybersecurity and AI/ML. Discover how innovation is revolutionising the way we protect our digital world through insightful talks, keynote sessions and networking!

Building on the success of the two previous AMLUCS conferences in 2023 and 2024, we will be hosting the third AMLUCS conference on the 9th and 10th September 2025 at We The Curious, Bristol Science Centre.

Key Dates

Key dates and deadlines for submissions to AMLUCS 2025 are as follows:

- 7th April 2025 – Call for Submissions released
- 9th June 2025 – Submission deadline
- 30th June 2025 – Notification of outcome
- 21st July 2025 – Draft content deadline
- 18th August 2025 – Content finalised
- 9th – 10th September 2025 – AMLUCS 2025 conference

Format

Last year's format was well received, so we will continue with presentations on the main stage with posters available to view during scheduled poster sessions and breaks.

Themes

We are inviting submissions against the following themes but are open to alternative ideas. If you feel your research is relevant but doesn't align to these themes, please contact amlucs@fnc.co.uk with an outline of your idea and we can discuss.

AI/ML Innovations & Applications in Cyber Defence

- AI-assisted situational awareness and threat intelligence, including, but not limited to, forensics, attack attribution and attack path forecasting
- Automated cyber incident response & recovery
- Deception and decoy techniques for cyber defence
- Leveraging foundation models for cyber defence, including large language models (LLMs)

Defending against AI/ML-driven attacks

- Threat emulation and automated vulnerability testing
- Novel approaches specific to defence against AI/ML-driven attacks
- Combatting cyber-related information operations including deepfakes

Improving AI/ML Training

- Realistic cyber defence training & testing environments
- Training in a data-poor cyber environment

Human Augmentation

- Human-machine teaming or other human sciences approaches related to the intersection of AI/ML and cyber security
- AI/ML tools for enhancing the cyber training of humans including green agent pattern of life or other enablers for exercises (cyber range or tabletop), wargaming, or simulated scenarios

Safety & Security of AI/ML

- Responsible, ethical, trustworthy & fair AI/ML
- Latest applied explainability approaches (i.e. beyond SHAP)
- Approaches for improving the security of AI/ML, particularly reinforcement learning and foundational models, including LLMs

To broaden our horizons and support wider participation in 2025, non-Defence use cases are encouraged (Defence research is still very welcome). Research related to cyber-physical systems will also be viewed positively. Registration is not a pre-requisite for submission.

Submission Process

1) Abstracts must be submitted to the amlucs@fnc.co.uk inbox and no more than 500 words per submission. Abstracts should introduce your research, its aims, benefits and key findings to date.

2) Additionally, submissions should also include the following supporting information:

- Responses to each of the three assessment criteria (listed at #3 below - no more than 100 words per criteria)
- Your favourite aspect of the work, and why (no more than 100 words)
- The theme(s) you believe the work is aligned to (see above)
- Whether you would like to be considered for a poster and/or a presentation (you can be considered for both)
- Research funding route
- Previous presentations, publications and submissions related to your AMLUCS submission (research submitted elsewhere is not excluded)
- A clear explanation of the application of generative AI in preparation of your submission and underpinning research (if applicable) [1]

3) The abstracts will be reviewed by our technical committee and down selected for the event, at which point successful applicants will be notified. Submissions will be assessed against three top-level criteria:

- Innovative & rigorous [2] application of ML methods
- Cybersecurity impact
- Submission quality and audience appeal

4) Successful applicants will be requested to submit a full submission of their presentation and/or poster. The technical panel will review submissions, provide feedback (if required), and provide final approval. Please be aware that MOD funded research will be required to follow the Permission to Publish (P2P) process. The AMLUCS team will assist you with this process.

[1] - The use of Generative AI tools is permitted to assist in writing or research. However, authors take full responsibility for all content in their submission, including any content generated by AI.

[2] - As a minimum we ask that interpretable benchmark(s) are included to gauge the research benefits. Preferred benchmarks include rules-based human expert logic, tuned PPO agents or other applicable standard approaches. Further benchmarks to define the performance envelope will be viewed favourably e.g., green agent only (i.e. normal users), attacker with no defender and visa versa.

Conference Context

Presentations

30-minute presentations will be conducted in-person, with 20 minutes to present and 10 minutes for Q&A.

The presentation should introduce your research, its aims, benefits and the findings to date with application, if applicable. Slides will be made available to attendees after the conference.

Posters

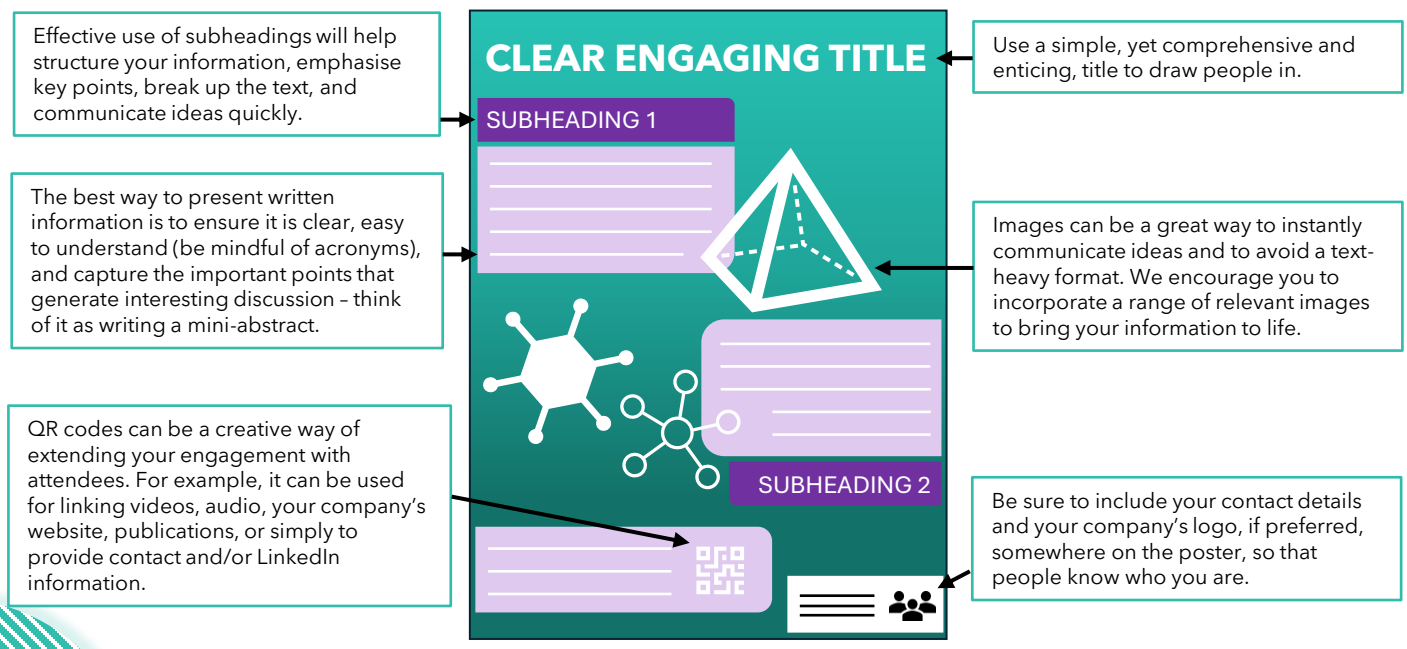
Posters will be displayed throughout the conference space, with time dedicated in the agenda for attendees to view them. The use of diagrams and images is encouraged, and the following content is suggested:

- Problem (situation, complication and research question(s))
- Approach (answer to the problem)
- Benefits (if possible, quantified) and outcomes (including key achievements)
- Exploitation routes and opportunities
- Impact of work (e.g. growth of cyber / AI skills, internal investment , recruitment, etc.)

Poster authors will be required to attend. You will need to print your own poster on size A0 paper, with a suggested minimum text size of 18. The poster can be portrait or landscape.

Example Poster Layout

An example poster format is shown below. Further guidance will be released upon acceptance.



AMLUCS

APPLIED MACHINE LEARNING FOR CYBER SECURITY

Contact Us

For general questions and enquiries, please contact us at: amlucs@fnc.co.uk